Report of the Director of Policy and Resources

Decision to be taken after 5 April 2013

NORTH LINCOLNSHIRE COUNCIL

CABINET MEMBER POLICY & RESOURCES

INFORMATION GOVERNANCE FRAMEWORK POLICY

1. OBJECT AND KEY POINTS IN THIS REPORT

1.1 To consider and approve an updated Information Governance Policy Framework (formerly known as the Information Management Policy).

1.2 The key points in this report are as follows:

- Our preparations for NHS public health transition require the council to strengthen its information governance arrangements.
- Our vision is to be a dynamic, high performing customer focused council, giving the best possible value for money and changing outcomes for all people living and working in North Lincolnshire.
- Developing a robust information governance framework is key to protecting the integrity of our vision.
- An information governance framework has been developed which sets out the framework and strategic direction for all activities relating to information governance.

2. BACKGROUND INFORMATION

2.1 The council currently has an over-arching information management policy that sets out the principles for managing all information assets and application of regulatory frameworks and standards for managing data and information across the council.

2.2 Adopting a framework approach to information governance is a key requirement to ensure we meet our obligations arising through the NHS public health transition arrangements. To this end our Information Management policy has been revised accordingly and as an over-arching policy now includes a range of activity for managing and monitoring the policies, processes and procedures it contains.

2.3 The importance of information governance needs to be reinforced across the workforce. The revised policy will be issued to key staff who have been allocated information governance roles and responsibilities.

2.4 The benefits of pursuing information governance include:

- Demonstrate effective and efficienct management of a key corporate asset
- Minimise the risk of financial damages arising through an information security breach.
- Protect the reputation of the council.
- Proactively comply with the changing environment for local authorities in relation to obligations enforced by the Information Commissioner.

2.5. The policy is a 'live' document and will be kept under constant review to ensure it remains fit for purpose and facilitates the council in achieving its vision efficiently and securely. The policy sets out a framework and includes arrangements for the following:

- Management of information with key roles and responsibilites
- Confidentiality and Data Protection assurance
- Information Security assurance
- Data Quality assurance

2.6. The policy also includes a suite of individual key policies of which one is new, and threehave been revised:

- New – Records Management Policy
- Revised – Data Protection Policy
- Revised – Freedom of Information Policy
- Revised – Environmental Information Regulations Policy

3. OPTIONS FOR CONSIDERATION

3.1 Option 1 – Approve the Information Governance Policy Framework and the four policies

3.2 Option 2 – Do not approve the information security policy and request changes be made.

4. ANALYSIS OF OPTIONS

4.1 Option 1 – Approving the policy would provide a clear framework for assuring our partners of our good management practices and also assure ourselves that to comply with our legal responsibilities we constantly review our policies and procedures. Approving the policy would also ensure the council is complying with the NHS public health transition arrangements. Robust information governance arrangements are essential for protecting the personal data of local residents and service users.

4.2 Option 2 – Not approving the policy at this time could result in a delay in complying with the NHS public health transition arrangements or cause a

disruption to the way that Public Health currently work when they move to the council.

5. RESOURCE AND OTHER IMPLICATIONS (FINANCIAL, STAFFING, PROPERTY, IT)

5.1 Key staff with information governance responsibilities will be required to read and accept the conditions of the policy. They will also be instrumental in helping to implement the policy. No extra resources will be needed as the Policy and Resources directorate will lead and work with other directorates on the implementation.

5.2 Failure to comply with information governance legislation can result in the Information Commissioner imposing fines of up to £500,000. In addition the reputation of the council would be affected as a result of any negative publicity.

6. OTHER IMPLICATIONS (STATUTORY, ENVIRONMENTAL, DIVERSITY, SECTION 17- CRIME AND DISORDER, RISK AND OTHER)

6.1 An integrated impact assessment has been undertaken and impacts identified have helped shaped the policy. Both the policy and the integrated impact assessment will be kept under constant review.

7. OUTCOMES OF CONSULTATION

7.1 Consultation has taken place with the council management team, the Information, Improvement & VFM Group, legal services, IT, internal audit, and directorate co-ordinators as appropriate to develop this policy.

8. RECOMMENDATIONS

8.1 That the cabinet member approves the information governance policy framework

DIRECTOR OF POLICY AND RESOURCES

Civic Centre
Ashby Road
SCUNTHORPE
North Lincolnshire
DN16 1AB

Author: Chris Daly

Date: 4 March 2013

Information Governance Policy Framework

March 2013

Lead Officer: Chris Daly, Head of Information Management

Document History

Purpose	
Document Purpose	To provide a corporate governance framework for Information Governance within the Council and for sharing information and data with other agencies
Document developed by	Head of Information Management
Document Location	This document is located on the council's Web site and on the network at: *\\Pittwood\scco\Information Management\IM Policy\2013 Policy\IM Policy Refresh March13 v2.3 final draft.doc*

Revision	
Revision date	**13th March 2013**
Version	1
Status	Approved
Summary of changes	Completely revised in line with the NHS's framework requirements, and includes roles and responsibilities, and assurances on confidentiality, information security, and data quality. The implementation action plan also contains NHS self-assessment actions required to reach level 2.

Approvals	
Head of Information Management	Lead the review of the framework and policies
Assistant Director, Business Support	Oversee the document through the council's approval process
Improvement & VFM Group	Approve the Framework and changes made recommending adoption to CMT
Cabinet	Approve the review of the framework and policies

CONTENTS:

1. Introduction

The council generates and receives an enormous amount of information. It therefore acknowledges that information is one of its key corporate assets and as such requires the same discipline to its management as is applied to its other important corporate assets such as finance, people and property. Information assets include all paper archives, paper based case files, current paper records, electronically held records in back-office systems, network drives and within email systems.

Good information management is vital in ensuring the effective and efficient operation of services, meeting security standards and legislation, as well as demonstrating accountability for its decisions and activities. In order to maximise the effective and efficient use of its information it is crucial that the council has a corporate view on how to manage the creation, storage, retrieval, retention, disposal and sharing of information effectively and consistently across the organisation.

This framework policy sets out roles and responsibilities, policies and procedures, along with best practice and standards for managing our information assets. It also describes our approach to assurance and risk management.

1.1. Purpose

To set out the council's responsibilities and activities in relation to information governance in accordance with legislation and professional principles.

The policy summarises the relevant regulations and commits the council to their application where appropriate. It has been updated to take into account the standards required by the NHS in respect to the transition of Public Health to the council in April 2013, and as such is presented as a framework comprising three elements:

- The corporate management of information governance
- An overarching policy drawing all the legislation and issues together
- A suite of comprehensive individual policies

1.2. Scope

This policy applies to officers and services of the Council and all elected members whilst they are working on council business,. The council has a duty to schools and as such they are welcome to adopt this approach.

It applies to all information assets irrespective of their format:

- In the case of the Data Protection Act 1998 (DPA) it applies to all personal data acquired, held and used.
- In the case of the Freedom of Information Act 2000 (FOI) it applies to all recorded information held, including that on network drives and within the email system.

- In the case of Environmental Information Regulation 2004 (EIR) it applies to all environmental information held by the council or by the council on behalf of someone else, in written, visual, aural, electronic or other material form.

Contractors are included in the policy, but there are some exclusions such as the voluntary sector, care home providers, nurseries, child minders, etc. However, all contractual arrangements will include a section detailing the council's Information Management compliance requirements.

1.3. Aims and Objectives

The aim of information governance is to achieve excellence in the management of council records and information assets. The key objectives are to:

- Build an information governance culture where information and records are managed coherently and consistently across the council. Roles and responsibilities are set out and supported by skills, knowledge and experience.
- Develop clear guidance for staff by developing a continuous training plan, which sets out competencies for staff and the various ways to access training. This will be discussed in Employee Appraisals and during Induction for new staff.
- Maintain confidentiality and data protection assurance by ensuring Data Protection principles are inherent throughout the council, and that there is clear guidance and training for staff. Requests for information will be appropriately dealt with. All contracts specify compliance requirements.
- Be open and transparent by keeping the Publication Scheme up-to-date and responding to requests for information as mandated by the government. Also documented procedures for FOI and EIR will be available to the public.
- Share Data where appropriate ensuring proper protocols are designed and managed. Confidentiality of service users is protected through the use of pseudonymisation and Anonymisation techniques, which ensures that individuals cannot be re-identified. The Humber Information Sharing charter sets out rules agreed by public bodies within the Humber Region.
- Manage records using good practice standards including identifying vital records and their systems ensuring they are protected, i.e. those required to maintain business continuity in the event of a disaster and without which the council could not operate.

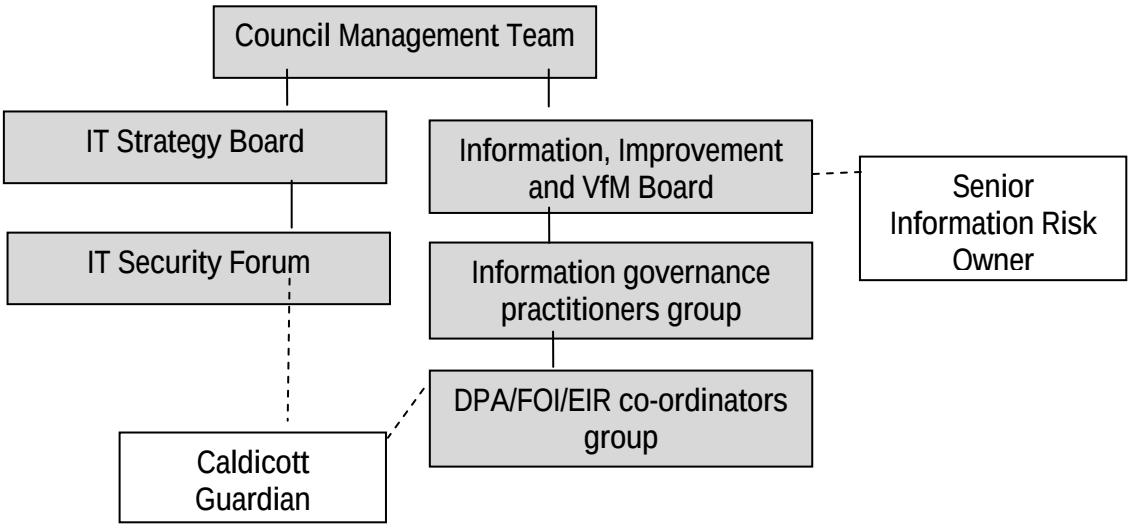
1.4. The regulatory environment

There has been an increasing emphasis on the importance of information in the public sector, which has influenced a more robust regulatory framework.

- The Data Protection Act (DPA) is there to guide and help us ensure that we do the right thing by our citizens when we hold personal information and data about them.
- The Freedom of Information Act stems from the intention to make information about government and its decisions open and transparent.
- The Environmental Information Regulation stems from the intention to make environmental information open and transparent.
- The government Transparency Agenda brings new challenges for making data more accessible to the wider community.

2. Information Governance Management

The council has an information governance agenda, which is led by a comprehensive action plan built up from reviewing and monitoring the policies and processes on a regular basis. There are several key governance bodies identified within the framework, which meet to review and monitor action plans. The Director of Policy and Resources leads the overall activity.



2.1. Information as a corporate asset

1. The council will maintain an inventory of its information assets.
2. Information is made available unless there is a compelling reason not to, recognising all the relevant legislative and regulatory requirements. This applies to both internal and external users of information. Efforts are made to present and organise information to maximise its availability.
3. The storage and organisation of information will promote its sharing, thereby minimising duplication of effort and the cost of its retrieval. An aspiration to pull all intelligence from information sources into one place will aid decision making.
4. All information will have a defined owner(s). It will be their responsibility to manage, protect and to make it available to others.
5. The protection of information assets is carried out in accordance with council's Information Security Policy.
6. The management and retention of information will take into account its value to the council. Information will only be retained as long as there is a business need and to ensure compliance with the relevant legal and regulatory requirements.
7. Disposal of information of a personal or confidential nature will be carried out securely and when there is no longer a legal or business need to keep it.
8. Information ownership rights will be observed in that Information from third party sources will only be used in accordance with the licence or permissions granted.

2.2. Compliance with the Freedom of Information (FOI) Act 2000

Public authorities have two main responsibilities under the Act. They have to produce a Publication Scheme (effectively a guide to the information they hold that is publicly available) and they have to deal with individual requests for information.

In order to fully comply with the Act, the council requires the ability to know that the information being requested exists and to be able to locate it promptly. Generally, such requests need to be responded to within 20 working days and this can only be achieved if information is being well managed.
See Appendix 1 for FOI Policy.

2.3. Compliance with the Environmental Information Regulations (EIR) 2004

The council will comply fully with the EIR, which give the public a right of access to environmental information held by a public authority, other than that which is exempt. Generally such requests need to be responded to within 20 working days.

Public authorities have two main responsibilities under the Regulations. They have to actively disseminate environmental information and they have to deal with individual requests for information.
See Appendix 2 for EIR Policy.

2.4. Corporate Records Management

The council recognises that its records are an important public asset and are available to those who are entitled to see them. They are a key resource for the effective operation and accountability of the council. Like any other asset, they require careful management and the Records Management Policy sets out the council's responsibilities and activities to do this. The council also recognises that some of its records will, over time, become of historical value and as such need to be identified and preserved accordingly.
See Appendix 3 for Records Management Policy

2.5. Review and monitoring

This framework policy and the supporting standards will be monitored and reviewed regularly in line with legislation and codes of best practice, reporting to the Information, Improvement and Value for Money Board for strategic direction and approval.

A performance-monitoring framework is established to evaluate the effectiveness and efficiency of Information Governance activities across the council.

2.6. Complaints

The council will ensure that its services are as efficient and effective as possible. If people feel that their request has not been dealt with in a satisfactory manner it will be reviewed using the council's FOI, DPA and EIR Complaints Policy, details of which are located on the council's website.

Where the complaint is not about a breach of the act or regulations we aim to resolve the issue informally and the Service co-ordinator(s) for FOI, DPA, EIR will do all they can to put things right.
See appendix 4 for the Complaints Policy.

2.7. Roles and responsibilities

Responsibilities for information governance are assigned to specific staff and this is written into employment contracts. An annual training plan identifies various levels of training for all staff setting out the organisation's expectations for working practices and behaviours related to information governance. Guidance and information is available to staff on all aspects of information governance, which is available on the council's web site.

Specific roles and responsibilities have been assigned to various staff to undertake information governance activities across their service areas. Via a corporate lead, this will enable services to take the necessary ownership whilst ensuring the promotion, development and implementation throughout the organisation.

- **Senior Information Risk Owner (SIRO)**

The SIRO is concerned with the management of all information assets and is a senior officer familiar with information risks and leads the organisation's response. This role is the focus for the management of information risk and reports to the Improvement and Value for Money Group. The SIRO is accountable, fosters a culture for protecting and using data and provides a focal point for managing information risks and incidents.

This role is built into the job description of the Head of Business Improvement and Information Governance.

- **Information Governance & Data Protection Officer (IG&DPO)**

The IG&DPO deputises for the SIRO and works as the corporate operational lead to ensure the promotion, development and implementation of information governance policies. The IG&DPO is the council's nominated Data Protection Officer and co-ordinates the needs of Data Protection across the council.

This role is built into the job description of the Principal Information Governance Officer.

- **Caldicott Guardian**

The Caldicott Guardian is concerned with the management of Service User information. The Caldicott Guardian is a senior social services practitioner within the People Directorate. The role is advisory; is the conscience of the Directorate and provides a focal point for Service User confidentiality and information sharing issues.

- **Information Asset Owner (IAO)**

IAO's are concerned with the information used within the running of their particular area of business. They are senior individuals and their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result they are able to understand and address risks to the information, and ensure that information is fully used within the law for the public good, and provide written input to the SIRO annually on the security and use of their asset.

This role is built into the job descriptions of various senior officers in the council – see Appendix 6 for list of co-ordinators.

- **Data Protection / FOI / EIR co-ordinators**

Each Service has nominated co-ordinators for Data Protection, FOI and EIR who are responsible for co-ordinating responses to FOI requests and DPA Subject Access Requests (SAR's) for their service area.

- **Records Co-ordinators**

Each Service is assigned a Records co-ordinator and it is their responsibility to ensure records are managed in line with the Records Management Policy. They will ensure records are stored in proper conditions and retained according to retention rules and are disposed of accordingly.

- **All employees**

All employees and those acting on behalf of the council are responsible for the data and information they generate. All staff will be made aware of their responsibilities and in particular of the DPA, FOI and EIR and the duties they place on the council as a public authority.

3. Confidentiality and Data Protection Assurance

3.1. Data Protection

The council is fully committed to compliance with the requirements of the Data Protection Act 1998. A policy and well-designed procedures have been developed that aim to ensure that all employees, elected members, contractors, partners or other servants of the council who have access to any personal data held by or on behalf of the council abide by their duties and responsibilities under the Act.

The policy applies to all personal information held by the council or held on behalf of the council. This includes information on paper and in electronic formats, including personal information collected by CCTV cameras.

There are other relevant statutory UK and EU legislation that have links to Data Protection and these are cited in the Policy.
See appendix 5 for the Data Protection Policy.

3.2. Collecting and using information

The council is very clear that personal information shall only be used where there is a lawful basis to do so and objections to the disclosure of confidential personal information shall be appropriately respected. There are various Privacy Statements in use to inform individuals about the proposed uses of their personal information. There is a Privacy Statement on the council's web site and a specific one for the electronic request for services via the self-service portal. All paper data collection forms have a privacy statement.

3.3. Sharing Information

The council is committed to using and sharing data in order to carry out its duties to the people of North Lincolnshire, it recognises the importance of confidentiality to service users. Along with the other public sector agencies within the Humber region the council has agreed to a Humber Sharing Charter, which has been adopted as policy by the council and signed up to by the Chief Executive. When the council is working with its partners they will each agree whether they are giving consent to share their data with each other and they will draw up a specific data sharing protocol in accordance with the Charter.

Data sharing protocols follow a three tier model:

- **Tier 1** – a high level charter that establishes the ***Principles*** and standards for information sharing
- **Tier 2** – a set of ***Protocols*** which agree the ***Purposes*** for which information will be shared
- **Tier 3** – a set of specific agreements that define the ***Processes*** by which information can and will be shared, and with whom.

The council has a process for determining if and how to share data along with templates for setting out Tiers 2 and 3. All data sharing will be approved by senior management and logged in the corporate Data Sharing Register. Training will be designed for staff.

Responsible managers for each agency, organisation or the council, have overall responsibility for any Information Sharing protocols into which they enter. Staff of these partnerships who work directly with the Service Users in order to carry out the functions described in the protocol are bound by the document and as such, along with the council will ensure that all staff, current and newly employed, whether temporary, voluntary or seconded, receive training with respect to the data sharing responsibilities and in particular, the Data Protection Act..

See appendix 6 for Humber Information Sharing Charter.

4. Information Security Assurance

4.1. Information Security

The council expects to protect its information assets from all threats whether internal or external, deliberate or accidental. The Information Security Policy sets out the controls and requirements to do this. The purpose of security in an information system is to preserve an appropriate level of:

- **Confidentiality:** to prevent unauthorised disclosure of information
- **Integrity:** to prevent the unauthorised amendment or deletion of information
- **Availability:** to prevent unauthorised withholding of information or resources

As with all policies staff will be required to agree to the requirements of the policy and be required to undertake specific training.
See appendix 7 for Information Security Policy

4.1.1. Skills and knowledge

It is important to the council that staff has the skills and knowledge to properly look after the information in their trust. Roles and responsibilities have been assigned for all the information governance elements and guidance and training is given to staff. A continuous Training Plan sets out requirements and the various ways to access training. Training is discussed during Employee Appraisals and during the Induction process for new staff.

4.1.2. Office and Desk security

The council maintains a clear desk policy to help ensure that all personal and sensitive information is not left unattended and is stored securely when not in use. A Confidential Waste policy determines that confidential waste is kept in a secure place until it can be collected for secure disposal via the council's corporate confidential waste facility.

4.1.3 Information data flows

The council will ensure that all transfers of hardcopy and digital personal information are identified and a corporate register of data flows is maintained.

4.1.4. Anonymisation and pseudonymisation of data

Confidentiality of service user information is protected when appropriate through the use of pseudonymisation and anonymisation techniques, which turn data into a form which does not identify individuals and where re-identification is not likely to take place. This is particularly relevant in services providing business intelligence to other agencies, for example Public Health's role.

4.2. Risk Management

There can be significant risks in not managing information appropriately and this can have consequences for both the council's reputation and its finances. There have been numerous cases where public authorities have failed to manage their information properly, which have resulted in significant consequences for both the organisation and the individuals they serve.

The council will provide protection by managing risks to the confidentiality, integrity and availability of information to assist our business to function effectively.

- Confidentiality means ensuring that only authorised people can access information
- Integrity means ensuring that it is authentic, accurate and complete
- Availability means that authorised people can access it when they need to, at the right times in the right ways

Information Governance is logged as a strategic Risk at the highest level. Risks are continually being considered, particularly at the Information Security Forum and the various groups that come together to manage the implementation plan. All risks are logged on the corporate Risk Register and are formally reviewed quarterly.

4.3. Network Management

The council's network is segmented to protect sensitive council information systems from unauthorised access via Internet, wireless and internal based access. Secure firewalls, and other controls such as Virtual Private Networks, are used to control remote access across the Internet. IT Services also use other appropriate technologies e.g. secure firewalls, Virtual LANs and routers, to segregate the internal network where necessary.

Secure network connection controls are in place, i.e. firewalls and routers, between the council and any other organisation's network, including the Internet. The controls are configured to restrict access in line with the council's business and security requirements.

Network routing controls are implemented so that computer connections and information flows are restricted in line with the council's business and security requirements.

4.4. Incident management

Every care is taken to protect personal data and to avoid a data protection breach, however, in the unlikely event of a breach, or of data being lost, it is vital that appropriate action is taken to minimise any associated risk as soon as possible.

The council has a Data Breach Policy and a Breach Management Plan for such circumstances, ensuring that a standardised management approach is implemented throughout the council.

See appendix 8 for Data Breach Policy

In cases where an IT system is breached that would compromise Data Protection an IT Security Incident Response Team will be formed to address the incident.

4.5. Information systems control

A corporate Information Asset register is maintained, which contains key information such as software, hardware and services. The Head of IT will ensure that information systems are checked regularly for technical compliance with relevant security implementation standards, which are documented in the Information Security Policy.

Information Asset Owners are responsible for ensuring that the systems in their Services, both electronic and paper based are documented on the asset management register and that they have appropriate controls and procedures in place. Responsibility for defining and documenting requirements for both system and user access controls have been assigned to appropriate staff.

4.6. Business Continuity Plans

The council's business continuity plans are continuously reviewed. IT service continuity management (ITSCM) covers the processes by which plans are put in place and managed to ensure that IT Services can recover and continue even after a serious incident occurs. It is not just about reactive measures, but also about proactive measures – reducing the risk of a disaster in the first instance.

5. Data Quality Assurance

5.1 Data Quality

The council recognises that the quality of the data that it holds is key to delivering effective and efficient services and requires data that is 'fit for purpose', i.e. having the right set of correct information at the right time in the right place for people to make decisions to run the council business, to serve customers and to achieve council goals. Information will be a trusted source for any/all-required uses meeting statutory and legal requirements. To this end there is a robust programme of internal and external data quality audit.

The council has an established corporate Data Quality policy to support its Performance Management System (PMS) in provision of Performance Information. This puts in place controls on the processes to collect data for and generate the Performance Indicators.

See appendix 9 for Data Quality Policy

5.2 Care Records Assurance

There is a documented strategy for maintaining the quality of the Social Care Service, which includes robust data recording standards. As part of the Striving for Excellence Improvement Plan, professional social care staff are involved in validating information derived from the recording of care activity.

Staff are trained and regularly appraised with respect to data integrity of Service User information and the quality audit system practiced in the People Directorate has regular audits of personal records to ensure that records are complete and that case diary records are of a sufficient standard.

5.3 Secondary Use Assurance

Documented procedures are in place for using both local and national benchmarking to identify data quality issues and analyse trends in information over time, ensuring that large changes are investigated and explained.

6. Improvement Plan

The council has identified four key themes for improvement: using the acronym E.D.G.E. under which a detailed action plan can be put together to deliver this policy:

Exploiting information resources
Delivery of Data Quality
Governance
Education and best practice

7. Information Governance Policies

7.2. A suite of policies and procedures supports the framework.

Section In Framework	Policy	Date Approved	Date Revised\ approved
2.2	Freedom of Information Policy	December 2011	March 2013
2.3	Records Management Policy	March 2013	
2.5	Complaints Policy	June 2013	
3.1	Data Protection Policy	December 2011	March 2013
3.4	Information Sharing Charter	March 2012	
4.1	Information Security Policy	January 2013	
4.4	Data Breach Policy	June 2013	
5.1	Data Quality Policy	August 2011	

8. Appendices

Appendix 1 Freedom of Information Policy
Appendix 2 Environmental Information Regulations Policy
Appendix 3 Records Management Policy
Appendix 4 Complaints Policy
Appendix 5 Data protection Policy
Appendix 6 Humber Information Sharing Charter
Appendix 7 Information Security Policy
Appendix 8 Data Breach Policy
Appendix 9 Data Quality Policy

1 COUNCIL Putting our CUSTOMERS 1ST

Freedom of Information Act Policy

NORTH LINCOLNSHIRE COUNCIL

www.northlincs.gov.uk

Document History

Purpose	
Document Purpose	To provide a corporate policy for Freedom of Information Act
Document developed by	Head of Information Management
Document Location	This document is located on the council's web site and on the network at: *C:\DOCUME~1\CHRISD~2\LOCALS~1\Temp\Domino Web Access\IM Policy Refresh March13 v2.1.doc*

Revision	
Revision date	**07 March 2013**
Version	1
Status	Approved
Summary of changes	Completely revised in line with the NHS's Information Governance framework requirements.

Approvals	
Head of Information Management	Lead the review of the framework and policies
Assistant Director, Business Support	Oversee the document through the council's approval process
Improvement & VFM Group	Approve the Framework and the Freedom of Information Act Policy and any changes made, recommending adoption to CMT
Cabinet	Approve the review of the framework and policies

Contents Page

1. Introduction

The Freedom of Information Act 2000 came into force in England, Wales and Northern Ireland in January 2005. The Information Commissioner's Office (ICO) regulates the Freedom of Information Act in the UK and a copy of their guidance note about this legislation can be accessed at www.ico.gov.uk.

The council already makes a considerable amount of information available to the public via its website, local link offices, council offices, leisure centres, tourist information offices, local newspapers and libraries.

The council's constitution sets out the basis of the public's right to information held by the council and to information on council decisions and the reasons for those decisions. Information is an important asset that the council manages and Freedom of Information provides a catalyst to make it more widely available.

The Freedom of Information Act gives a general right of access to both individuals and organisations to all types of recorded information held by public authorities. The council is considered to be a public authority under the Act. Recorded information includes paper records, emails, information stored on computer, audio or videocassettes, microfiche, maps, photographs, handwritten notes or any other form of recorded information. Information that is known to officials but not recorded is not covered by the Act.

Public authorities have two main responsibilities under the Act. They have to produce a Publication Scheme (effectively a guide to the information they hold which is publicly available) and they have to deal with individual requests for information. The Act also sets out exemptions from this right of access, whilst placing a number of obligations upon public authorities.

Generally, requests for information need to be responded to within 20 working days. Being able to satisfy requests for information requires the ability to know the information exists and to be able to locate it promptly. This can only be achieved if information is being well managed. The Lord Chancellor's "Code of Practice on the Management of Records" under section 46 of the Freedom of Information Act provides guidance on practices to be followed in order to comply with the Act.

All requests for information are recorded in a single corporate register with a unique identification reference number. They are managed using the Council's Firmstep Customer Relationship Management (CRM) system.

This policy is part of a suite of information governance policies.

2. Purpose

The purpose of this policy is to ensure compliance with the Freedom of Information Act. This will be achieved by ensuring that there is an up to date Publication Scheme and that requests for information are dealt with as set out in this policy and therefore as required by the Freedom of Information Act.

3. Scope

This policy applies to any information held by the council or by someone else on behalf of the council.

The scope of this policy extends to:

- Employees, contractors, volunteers, agencies and partner organisations operating on behalf of the council. ;
- Elected members in terms of information received, created or held by an elected member on behalf of the council. (Elected members are not authorities for the purposes of the Freedom of Information Act therefore any information held by an elected member for their own private, political or representative purposes is not usually covered by the Act and therefore this policy).

This policy does not apply to those schools with delegated powers, unless adopted by the governing body.

4. Legal Framework

The council must comply with all relevant statutory UK and European Union legislation, including the following that have links to the Freedom of Information Act:

- Human Rights Act 1998
- Data Protection Act 1998
- Environmental Information Regulations 2004
- Common law duty of confidence
- Copyright, Designs and Patents Act 1988
- Regulation of Investigatory Powers Act 2000
- Health & Social Care Act 2001
- Children Act 2004
- Equality Act 2010
- Re-use of Public Sector Information Regulations 2005
- Criminal Justice and Immigration Act 2008
- Crime and Disorder Act 1998.

5. Linkages with other policies and procedures

This policy is supported by other policies, standards and procedures. These include but are not limited to the following:

- Information Governance Framework Policy
- Data Protection Act Policy
- Environmental Information Regulations Policy
- Records Management Policy
- Information Request Charging Policy
- Information Request Complaints Policy
- CCTV Policy
- Human resources policies and procedures:
  - Recruitment
  - Employee induction
  - Disciplinary policy
  - Home working, lone working, remote working
- IT technical security standards
- Employee Code of Conduct
- The Humber Information Sharing Charter

6. Obligations Under the Freedom of Information Act

The Freedom of Information Act places two main obligations on public authorities.

The first is to proactively publish certain information through a Publication Scheme.

The second is that individuals or organisations have a right of access to recorded information held by the council or on behalf of the council. Information known but not recorded is not covered. It should be noted that the right of access is not to a document but to the requested information and that exemptions apply which may prevent the release of information.

Information is classed as being held by the council if:

1. It is held by the authority, otherwise than on behalf of another person, or
2. It is held by another person on behalf of the authority.

7. Publication Scheme

The council's Publication Scheme is a guide to the types of information that the council routinely publishes.

The council has adopted the Model Publication Scheme prepared and approved by the Information Commissioner's Office (ICO).

The scheme commits the Council to:

1. Proactively publish or otherwise make available as a matter of routine, information, including environmental information, which is held by the council and falls within the defined classes of information listed below;
2. Specify the information which is held by the council and falls within the defined classes of information;
3. Proactively publish or otherwise make available as a matter of routine, information in line with the statements contained within the scheme;
4. Produce and publish the methods by which the specific information is made routinely available so that it can be easily identified and accessed by members of the public;
5. Review and update on a regular basis the information the council makes available under the scheme;
6. Produce a schedule of any fees charged for access to information which is made proactively available;
7. Make the publication scheme available to the public.

The model publication scheme is available on the Council's website (www.northlincs.gov.uk/foi/publicationscheme/).

Classes of Information

As explained above the information in the council's Publication Scheme is divided into 7. classes of information, as set out in the ICO Model Publication Scheme. The classes are:

1. Who we are and what we do;
2. What we spend and how we spend it;
3. What our priorities are and how we are doing;
4. How we make decisions;
5. Our policies and procedures;
6. Lists and registers;
7. The services we offer.

Additional assistance is provided as to the definition of these classes in sector specific guidance manuals issued by the Information Commissioner and these can be accessed at www.ico.gov.uk.

The following information will not generally be published in the Publication Scheme:

1. Information the disclosure of which is prevented by law, or which is exempt under the Freedom of Information Act, or is otherwise properly considered to be protected from disclosure;
2. Information in draft form;
3. Information that is no longer readily available as it is contained in files that have been placed in archive storage, or is difficult to access for similar reasons.

8. Requests for Information

The Freedom of Information Act provides individuals and organisations from anywhere in the world with the right to request access to information, from a public authority. These are known within the council as FOI requests.

The requester does not have to state that a request is being made under Freedom of Information for it to be covered by this Act. Any request for information not able to be answered as part of normal day to day business will be treated as a potential FOI request. Requesters will be advised if it is decided to consider the request an FOI request and will be asked to put the request in writing if the initial request was made verbally.

If a request for information that should be handled under another information request regime or as a combination of regimes the requester will be advised. An example is when a request for the personal information of the requester is made under the Freedom of Information Act. In this instance the request would be considered under the Data Protection Act.

Following is a summary of this request process. Further information is available on the Information Commissioner's website at www.ico.gov.uk.

FOI requests for information:

- Must be in writing.
- Must provide enough information to determine the information required.
- Must be accompanied by the requesters name and either a postal or email address.
- Ideally state the format the requester would like to receive the information in.

The council may be entitled to refuse any requests on procedural grounds, such as when the above points are not complied with. Also requests considered vexatious or over the fee limit may also be refused.

Further details about the Freedom of Information Act fee limit and other charges that may apply to requests for information can be found the Information Request Charging Guidance document on the council's website at www.northlincs.gov.uk.

If we are able to release the requested information we will collate it and advise the requester that the requested information is held and provide a copy. Sometimes an exemption will prevent us from releasing the information and sometimes this exemption will mean that we cannot confirm or deny that the information exists.

If information can be released we aim to make it available as soon as possible after receipt of the request, but within 20 working days. The information provided will be in the format requested by the applicant, if this format is reasonably practicable.

If we are unable to provide some or all of the requested information because this information is exempt from disclosure we will explain in writing, aiming to do so within 20 working days. Sometimes in this instance we will be able to advise whether or not we hold the requested information.

We will provide advice with each request about how to make a complaint, and how to appeal to the ICO should be requester be unhappy with how we have handled the request for information.

9. Contact Details

All requests for information should be made in writing to Customer Services using the following contact details:

Website
Via the council's website by clicking the 'Contact Us' link on the home page: www.northlincs.gov.uk

Email
By email to inforequest@northlincs.gov.uk

Post
By writing to 'North Lincolnshire Council, Customer Services - Freedom of Information, Church Square House, 30-40 High Street, Scunthorpe DN15 6NL

Assistance Required
If you need help to make a request or to put your request in writing please contact one of our advisors at a Local Link Office – see the council's website or appendix B for Local Link details.

10. Exemptions

The Freedom of Information Act identifies 23 exemptions to the right of access to information and which therefore may prevent release.

There are nine exemptions that are 'absolute' either in whole or part. When this type of exemption applies the requested information does not need to be disclosed in any circumstances.

There are also nineteen 'public interest' exemptions that are subject to a 'public interest' test either in whole or part. This means that although an exemption applies, the council may be required to release the information unless it considers the public interest in not disclosing, is greater than the public interest in disclosing.

There are ten 'public interest' exemptions that are also subject to a prejudice test, which must be carried out before the requested information can be considered exempt. This test will consider whether harm will or is likely to be caused if the information is released.

In some cases if an exemption applies and permits it we may also decide to 'neither confirm or deny' that we hold the requested information. This will happen when, for example if it would be damaging to even confirm or deny information exists.

More information about exemptions can be found in Appendix A.

11. Compliance with the Freedom of Information Act

The council will, through appropriate management ensure that all employees are aware of the Freedom of Information Act and the rights of individuals or organisations under this Act, by use of strict criteria and controls:

1. Ensure that records are managed in line with The Lord Chancellor's "Code of Practice on the Management of Records" under section 46 of the Freedom of Information Act, so that requests for information can be promptly responded to;
2. Ensure the quality of information created, used and held;
3. Ensure that there is a up to date Publication Scheme;
4. Ensure that individuals are aware of their rights under the Act and that they are able to exercise them;
5. Only apply exemptions as permitted by the Act.
6. Ensure that any third parties contracted by the Council adhere to appropriate controls in respect of the council's obligations under the Act;
7. Investigate and respond to complaints in relation to the Act as set out in the Information Request Complaints Policy.

12. Roles and Responsibilities

Full details of the council's Information Governance roles and responsibilities are set out in the Information Governance Policy Framework. The following roles and responsibilities are specific to compliance with the Freedom of Information Act:

Principal Information Governance Officer (Data Protection Officer & Deputy SIRO)

The Principal Information Governance Officer is responsible for:

- Creating a process for handling requests for information under the Freedom of Information Act;
- Promoting compliance with this policy and therefore the Freedom of Information Act;
- Producing and publishing the council's Publication Scheme.
- Providing expert advice to Freedom of Information Co-ordinators and other council employees on compliance with this policy and therefore the Act;
- Leading complaint investigations in relation to the Act;
- Investigating non compliance with this policy.

Democratic & Legal Services are responsible for providing legal advice in respect of the FOIA.

Freedom of Information Co-ordinators

Each directorate/service is assigned a Freedom of Information Co-ordinator and it is their responsibility, over and above those responsibilities assigned to all employees, to:

- Process requests for information under the Freedom of Information Act;
- Assist managers with compliance with this policy and therefore the Act;
- Report any breaches or potential breaches of this policy to the Senior Information Risk Owner (SIRO) or Principal Information Governance Officer.

13. Complaints

The Council is determined to ensure that its services are as efficient and effective as possible. If people feel that their request has not been dealt with in a satisfactory manner it will be reviewed using the council's FOI, DP and EIR Complaints Policy, details of which are located on the website.

Complaints will be investigated by way of an internal review and we aim to ensure that the complainant receives a response within 20 working days.

Anyone not happy with the outcome or the handling of the council's internal review may seek an independent review from the Information Commissioner and requests should be made in writing to:

The Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Telephone: 01625-545700 / Fax: 01625-545510

14. Audit

The Freedom of Information Act policy, standards and procedures will be audited periodically as part of the annual internal audit work plan, to ensure compliance.

15. Monitoring and Review

The current version of this policy can be found on intralinc and the council website along with information supporting this policy. This policy and all supporting procedures will be reviewed as it is deemed appropriate but no less frequently than every 12 months.

Appendix A – Exemptions

Absolute Exemptions

1. Information accessible to the applicant by other means (section 21)
2. Security Matters (Section 23)
3. Court Records (Section 32)
4. Parliamentary Privilege (Section 34)
5. Conduct of public affairs (Section 36)
6. Communications with Her Majesty and awarding of honours (Section 37)
7. Personal information (Section 40)
8. Information provided in confidence (Section 41)
9. Other legal prohibitions on disclosure (Section 44)

Qualified Exemptions

1. Information intended for future publication (Section 22)
2. National security (Section 24) – prejudice based
3. Defence (Section 26) – prejudice based
4. International relations (Section 27(1)) – prejudice based
5. International relations – relating to information obtained from another state (Section 27(2))
6. Relations with the UK (Section 28) – prejudice based
7. The economy (Section 29) – prejudice based
8. Investigations and proceedings conducted by public authorities (Section 30)
9. Law enforcement (Section 31) – prejudice based
10. Audit functions (Section 33) – prejudice based
11. Formulation of government policy (Section 35)
12. The effective conduct of public affairs (Section 36) – prejudice based
13. Communications with Her Majesty – to the extent not absolute (Section 37)
14. Health and safety (Section 38) – prejudice based
15. Environmental information (Section 39)
16. Personal information – to the extent not absolute (Section 40)
17. Legal professional privilege (Section 42)
18. Commercials interests – which apply to trade secrets (Section 43(1))
19. Commercial interests (Section 43(2)) – prejudice based.

Appendix B – Local Link Office Details

Local Link Offices

Ashby Library & Local Link - Ashby High Street, Scunthorpe, DN16 2RY

Barton Local Link - Providence House, Holydyke, Barton, DN18 5PR

Brigg & District Local Link – The Angel, Market Place, Brigg, DN20 8LD

Crowle Community Hub - 52 – 54 High Street, Crowle, DN17 4DR

Epworth Library & Local Link - Chapel Street, Epworth, DN9 1HQ

Scunthorpe Local Link - Church Square House, 30 – 40 High Street, Scunthorpe, DN15 6NL

Winterton Library & Resource Centre - West Street, Winterton, DN15 9QJ

Environmental Information Regulations Policy

NORTH LINCOLNSHIRE COUNCIL

www.northlincs.gov.uk

Document History

Purpose	
Document Purpose	To provide a corporate policy for the Environmental Information Regulations
Document developed by	Head of Information Management
Document Location	This document is located on the council's web site and on the network at: *C:\DOCUME~1\CHRISD~2\LOCALS~1\Temp\Domino Web Access\IM Policy Refresh March13 v2.1.doc*

Revision	
Revision date	**07 March 2013**
Version	1
Status	Approved
Summary of changes	Completely revised in line with the NHS's Information Governance framework requirements.

Approvals	
Head of Information Management	Lead the review of the framework and policies
Assistant Director, Business Support	Oversee the document through the council's approval process
Improvement & VFM Group	Approve the Framework and the Environmental Information Regulation Policy and any changes made, recommending adoption to CMT
Cabinet	Approve the review of the framework and policies

Contents Page

1. Introduction

The Environmental Information Regulations 2004 came into force 01 January 2005, to fulfil the UK's legal obligations under European environmental directive 2003/4/EC.

The Information Commissioner's Office (ICO) regulates the Environmental Information Regulations in the UK and a copy of their guidance note about this legislation can be accessed at www.ico.gov.uk.

The council already makes a considerable amount of information available to the public via its website, local link offices, council offices, leisure centres, tourist information offices, local newspapers and libraries.

The council's constitution sets out the basis of the public's right to information held by the council and to information on council decisions and the reasons for those decisions. Information is an important asset that the council manages and Environmental Information Regulations provide a catalyst to make it more widely available.

The Environmental Information Regulations provide a right of access to environmental information held by a public authority to both individuals and organisations, and that environmental information is actively disseminated. The council is considered to be a public authority under the Regulations. 'Held' applies to information held by the public authority, held on their behalf or sometimes to information held on behalf of someone else. The Regulations also set out exceptions from the obligations to release information.

Environmental information is also sometimes available under other legislation or by public registers created as a result of other legislation.

The council is required under the Freedom of Information Act to produce and maintain a Publication Scheme (effectively a guide to the information they hold which is publicly available). This scheme will be used to actively disseminate environmental information.

Generally, requests for information need to be responded to within 20 working days, with an extension of up to 40 working days being permitted for complex or voluminous requests. Being able to satisfy requests for information requires the ability to know the information exists and to be able to locate it promptly. This can only be achieved if information is being well managed. The Lord Chancellor's "Code of Practice on the Management of Records" under section 46 of the Freedom of Information Act provides guidance on practices that will be followed with regard to environmental information.

All requests for information are recorded in a single corporate register with a unique identification reference number. They are managed using the council's Firmstep Customer Relationship Management (CRM) system.

This policy is part of a suite of information governance policies.

2. Purpose

The purpose of this policy is to ensure compliance with the Environmental Information Regulations. This will be achieved by ensuring that environmental information is regularly made available through the council's Publication Scheme and that requests for environmental information are dealt with as set out in this policy, and therefore as required by the Environmental Information Regulations.

3. Scope

This policy applies to any environmental information held by the council, held on behalf of the council or sometimes to that held on behalf of someone else.

The scope of this policy extends to:

- Employees, Contractors, volunteers, agencies and partner organisations operating on behalf of the council;
- Elected members in terms of information received, created or held by an elected member on behalf of the council. (Elected members are not authorities for the purposes of the Environmental Information Regulations therefore any information held by an elected member for their own private, political or representative purposes is not usually covered by the Regulations and therefore this policy).

This policy does not apply to those schools with delegated powers, unless adopted by the governing body.

4. Legal Framework

The council must comply with all relevant statutory UK and European Union legislation, including the following that have links to the Environmental Information Regulations:

- Human Rights Act 1998
- Data Protection Act 1998
- Freedom of Information Act 2000
- Common law duty of confidence
- Copyright, Designs and Patents Act 1988
- Regulation of Investigatory Powers Act 2000
- Health & Social Care Act 2001
- Children Act 2004
- Equality Act 2010
- Re-use of Public Sector Information Regulations 2005
- Criminal Justice and Immigration Act 2008
- Crime and Disorder Act 1998
- INSPIRE (Infrastructure for Spatial Information in the European Community) Regulations 2009.

5. Linkages with other policies and procedures

This policy is supported by other policies, standards and procedures. These include but are not limited to the following:

- Information Governance Framework Policy
- Data Protection Act Policy
- Freedom of Information Act Policy
- Records Management Policy
- Information Request Charging Policy
- Information Request Complaints Policy
- CCTV Policy
- Human resources policies and procedures:
  - Recruitment
  - Employee induction
  - Disciplinary policy
  - Home working, lone working, remote working
- Employee Code of Conduct
- The Humber Information Sharing Charter

6. Obligations Under the Environmental Information Regulations

The Environmental Information Regulations place two main obligations on public authorities.

The first is to actively disseminate environmental information.

The second is that individuals or organisations have a right of access to environmental information. This right is to environmental information held by the council, held on their behalf or sometimes on behalf of someone else. The right is to recorded information held in written, visual, aural, and electronic or any other material form, rather than to documents and only to information that exists at the time of the request. Information in someone's head that is not recorded is not covered.

Information is considered to be environmental information on:

a) The state of the elements of the environment – e.g. air, atmosphere, water, soil, land, landscape and natural sites such as wetlands, coastal and marine areas, biological diversity and the interaction of these elements;

b) Factors affecting (or likely to affect) the environment – including energy, noise, radiation, waste, emissions, discharges and other releases into the environment.

c) Measures – such as policies, legislation, plans, programmes, environmental agreements and activities affecting or likely to affect the elements and factors referred to above;

d) Reports – on the implementation of environmental legislation;

e) Economic analyses – including cost benefit and other economic analyses and assumptions used within the framework of measures and activities referred to in (c);

f) The state of human health and safety – including the contamination of the food chain, conditions of human life, cultural sites and built structures insofar as they are or may be affected by the state of the elements of the environment referred to in (a) or through those elements by any of the matters referred to in (b) or (c).

7. Publication Scheme

The council's Publication Scheme is a guide to the types of information that the council routinely publishes, including environmental information.

The council has adopted the Model Publication Scheme prepared and approved by the Information Commissioner's Office (ICO). More information is available in the council's Freedom of Information policy and the Publication Scheme is available on the council's website (www.northlincs.gov.uk/foi/publicationscheme/).

8. Requests for Information

The Environmental Information Regulations provide individuals and organisations from anywhere in the world with the right to request access to environmental information, from a public authority. These are known within the council as EIR requests.

The requester does not have to state that a request is being made under the Environmental Information Regulations for it to be covered by the Regulations. Any request not able to be answered as part of normal day to day business will be treated as a potential EIR request. Requesters will be advised if it is decided to consider the request an EIR request.

If a request for information that should be handled under another information request regime or as a combination of regimes the requester will be advised. An example is when a request for the personal information of the requester is made under the Environmental Information Regulations. In this instance the request would be considered under the Data Protection Act.

Following is a summary of this request process. Further information is available on the Information Commissioner's website at www.ico.gov.uk.

EIR requests for information:

- Can be verbal or in writing;
- Must provide enough information to determine the information required.
- Can be anonymous and do not have to provide contact details although these will usually be required in order for the council to respond.
- Ideally state the format the requester would like to receive the information in.

The council may be entitled to refuse any requests on procedural grounds, such as when the above points are not complied with. Also requests considered manifestly unreasonable may also be refused.

Further details about any charges that may apply to requests for environmental information can be found the Information Request Charging Guidance document on the council's website at www.northlincs.gov.uk.

If we are able to release the requested information we will collate it and advise the requester that the requested information is held and provide a copy. Sometimes an exemption will prevent us from releasing the information and sometimes this exemption will mean that we cannot confirm or deny that the information exists.

If information can be released we aim to make it available as soon as possible after receipt of the request, but within 20 working days or 40 working days for complex or voluminous requests. The information provided will be in written format but as far as is reasonably practicable will be in the format requested by the applicant.

If we are unable to provide some or all of the requested information because this information is exempt from disclosure we will explain in writing, aiming to do so within 20 working days.

We will provide advice with each request about how to make a complaint, and how to appeal to the ICO should be requester be unhappy with how we have handled the request for information.

9. Contact Details

All requests should be made in writing to Customer Services using the following contact details:

Website
Via the council's website by clicking the 'Contact Us' link on the home page: www.northlincs.gov.uk

Email
By email to inforequest@northlincs.gov.uk

Telephone
To the council's Contact Centre on 01724 297000.

Post
By writing to 'North Lincolnshire Council, Customer Services – Environmental Information Regulations, Church Square House, 30-40 High Street, Scunthorpe DN15 6NL

Assistance Required
If you need help to make a request please contact one of our advisors at a Local Link Office – see the council's website or appendix B for Local Link details.

10. Exceptions

The Environmental Information Regulations identify thirteen exceptions to the right of access to environmental information and which therefore may prevent release.

There is one 'absolute' exception and this applies to requests for personal information. When this type of exception applies the requested information does not need to be disclosed in any circumstances.

The other twelve exceptions are all subject to a 'public interest' test. This means that although an exception applies, the council may be required to release the information unless it considers the public interest in not disclosing, is greater than the public interest in disclosing.

The thirteen exceptions are divided into two categories based on either the type/nature of the information requested or the content of the information requested. Information on emissions into the environment is subject to more limited exceptions.

Under the Regulations there is an express presumption in favour of disclosure meaning that information should be made available unless there is a good reason for it not to be.

In some cases if an exception applies and permits it we may also decide to 'neither confirm or deny' that we hold the requested information. This will happen when, for example if it would be damaging to even confirm or deny information exists.

More information about both types of exemption can be found in Appendix A.

11. Compliance with the Environmental Information Regulations

The council will, through appropriate management ensure that all employees are aware of the Environmental Information Regulations and the rights of individuals or organisations under these Regulations, by use of strict criteria and controls:

1. Ensure that records are managed in line with The Lord Chancellor's "Code of Practice on the Management of Records" under section 46 of the Freedom of Information Act so that requests for information can be promptly responded to;
2. Ensure the quality of information created, used and held;
3. Ensure that environmental information is actively disseminated through the council's Publication Scheme;
4. Ensure that individuals are aware of their rights under the Regulations and that they are able to exercise them;
5. Only apply exceptions as permitted by the Regulations;
6. Ensure that any third parties contracted by the council adhere to appropriate controls in respect of the council's obligations under the Regulations;
7. Investigate and respond to complaints in relation to the Regulations as set out in the Information Request Complaints Policy.

12. Roles and Responsibilities

Full details of the council's Information Governance roles and responsibilities are set out in the Information Governance Policy Framework. The following roles and responsibilities are specific to compliance with the Environmental Information Regulations:

Principal Information Governance Officer (Data Protection Officer & Deputy SIRO)

The Principal Information Governance Officer is responsible for:

- Creating a process for handling of requests for information under the Environmental Information Regulations;
- Promoting compliance with this policy and therefore the Environmental Information Regulations;
- Producing and publishing the council's Publication Scheme;
- Providing expert advice to Freedom of Information/Environmental Information Co-ordinators and other council employees on compliance with this policy and the Regulations;

- Leading complaint investigations in relation to the Environmental Information Regulations;
- Investigating non compliance with this policy.

Democratic & Legal Services are responsible for providing legal advice in respect of the Environmental Information Regulations.

Freedom of Information/Environmental Information Regulation Co-ordinators

Each directorate/service is assigned a Freedom of Information/Environmental Information Regulation Co-ordinator and it is their responsibility, over and above those responsibilities assigned to all employees, to:

- Process requests for information under the Environmental Information Regulations;
- Assist managers with compliance with this policy and therefore the Environmental Information Regulations;
- Report any breaches or potential breaches of this policy to the Senior Information Risk Owner (SIRO) or Information Governance Officer.

13. Complaints

The Council is determined to ensure that its services are as efficient and effective as possible. If people feel that their request has not been dealt with in a satisfactory manner it will be reviewed using the Council's FOI, DP and EIR Complaints Policy, details of which are located on the website.

Complaints will be investigated by way of an internal review and we aim to ensure that the complainant receives a response within 20 working days.

Anyone not happy with the outcome or the handling of the council's internal review may seek an independent review from the Information Commissioner and requests should be made in writing to:

The Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Telephone: 01625-545700 / Fax: 01625-545510

14. Audit

The Environmental Information Regulation policy, standards and procedures will be audited periodically as part of the annual internal audit work plan, to ensure compliance.

15. Monitoring and Review

The current version of this policy can be found on intralinc and the council website along with information supporting this policy. This policy and all supporting procedures will be reviewed as it is deemed appropriate but no less frequently than every 12 months.

Appendix A – Exceptions

Regulation 12(3)

1) **Personal information.**
   Where the information requested contains personal information belonging to someone other than the requestor.

Regulation 12(4) - Refusal can be made if:

2) **Information is not held when the request is received.**
   Applies if the information is not held at the point the request is made, although it should be noted that it is an offence to destroy information after a request has been received in order to prevent release.

3) **Request is manifestly unreasonable.**
   For example, is vexatious or is so large as to be unreasonable. Where the request is too large the exception should only be used after an attempt has been made to offer assistance to create a more reasonable request.

4) **Request is too general.**
   This exception can only be used if an attempt has been made to help the applicant to refine or clarify their request.

5) **Information which is unfinished or in the course of being completed.**
   If this exception is used where information is intended for future publication the expected date of completion should be advised.

6) **Request involves the disclosure of internal communications.**
   This exception applies where there is a need to protect information created during internal thinking time.

Regulation 12(5) - Refusal can be made if disclosure would adversely affect the following:

7) **Disclosure would affect international relations, defence, national security or public safety.**
   Applies were harm could be caused by releasing the specified information.

8) **Disclosure would affect the course of justice, the ability of a person to receive a fair trial or ability of a public authority to conduct or criminal or disciplinary enquiy.**
   To apply this exception it must be shown that releasing the information would harm the course of justice or the right of an individual to a fair trial.

9) **Intellectual property rights.**
   Applies if the release of information could seriously damage the rights given under, for example trademarks and patents.

10) **The confidentiality of the proceedings of a public authority where such confidentiality is protected by law.**
This exception can only be used where confidentiality is protected by law not where information is simply marked ‘confidential’.

11) **Commercial or industrial confidentiality where such confidentiality is provided by law to protect a legitimate economic interest.**
Where such confidentiality is provided by law to protect a legitimate economic interest. To apply the exception it would need to be proven that the person or organisation would suffer a real commercial or competitive disadvantage if the information were released.

12) **The interests of the supplier of the information.**
Applies where the provider of the information did so voluntarily and was not under (and could not have been put under) a legal obligation to suuply the information and also did not give consent to its disclosure.

13) **The protection of the environment to which the information relates.**
Applies where releasing the information could have a detrimental affect on the environment.

Appendix B – Local Links

Local Link Offices

Ashby Library & Local Link - Ashby High Street, Scunthorpe, DN16 2RY

Barton Local Link - Providence House, Holydyke, Barton, DN18 5PR

Brigg & District Local Link – The Angel, Market Place, Brigg, DN20 8LD

Crowle Community Hub - 52 – 54 High Street, Crowle, DN17 4DR

Epworth Library & Local Link - Chapel Street, Epworth, DN9 1HQ

Scunthorpe Local Link - Church Square House, 30 – 40 High Street, Scunthorpe, DN15 6NL

Winterton Library & Resource Centre - West Street, Winterton, DN15 9QJ

1 COUNCIL Putting our CUSTOMERS 1ST

Records Management Policy

NORTH LINCOLNSHIRE COUNCIL

www.northlincs.gov.uk

Document History

Purpose	
Document Purpose	To provide a corporate policy for Records Management
Document developed by	Head of Information Management
Document Location	This document is located on the council's web site and on the network at: *C:\DOCUME~1\CHRISD~2\LOCALS~1\Temp\Domino Web Access\IM Policy Refresh March13 v2.1.doc*

Revision	
Revision date	**07 March 2013**
Version	1
Status	Approved
Summary of changes	Completely revised in line with the NHS's Information Governance framework requirements.

Approvals	
Head of Information Management	Lead the review of the framework and policies
Assistant Director, Business Support	Oversee the document through the council's approval process
Improvement & VFM Group	Approve the Framework and the Records Management Policy and any changes made, recommending adoption to CMT
Cabinet	Approve the review of the framework and policies

Contents ..... Page

1. Introduction

Information is a key corporate asset and the council creates, receives and handles vast amounts of it. It is vital that these assets are maximised through effective policies and procedures, to inform decision making, improve accountability, and enhance services to customers.

In order to maximise the effective and efficient use of its information it is crucial that the council has a corporate view on how it will manage the creation, storage, retrieval, retention, disposal and sharing of information effectively and consistently across the organisation.

There can be significant risks in not managing information appropriately. This can have consequences for both the council's finances and reputation. There have been numerous cases where public authorities have failed to manage their information properly. These have resulted in significant consequences for both the organisation and the individuals they serve, as for example council's have been fined for not looking after information adequately or have been criticised for not being able to supply information promptly in response to a Freedom of Information request.

This policy encompasses the management of all information assets, the understanding and the application of regulatory frameworks and standards for managing information across the council. It also sets out the roles and responsibilities for managing information across the council.

This policy is part of a suite of information governance policies.

2. Purpose

The purpose of this policy is to ensure that council records and information are managed appropriately. The key objectives of this policy are to:

- Build an information management culture where information and records are managed coherently and consistently across the council;
- Ensure compliance with legislation and standards;
- Collect information efficiently to support the council's objectives;
- Make better use of physical and electronic storage space;
- Ensure appropriate information is accessible when required;
- Ensure records are maintained in a safe and secure environment;
- Ensure records are kept for no longer than is necessary in accordance with the Retention and Disposal standards and disposed of or retained correctly;
- Ensure the council's vital records are identified and protected (i.e. those required to maintain business continuity in the event of a disaster, and without which the council could not operate);

- Make better use of employee time;
- Ensure employees are made aware of and receive appropriate training in records management.

3. Scope

This policy applies to all records and information held by the council or held on behalf of the council. This includes information on paper and in electronic formats, including information collected by the council's CCTV cameras.

The scope of this policy extends to:

- Employees, contractors, volunteers, agencies and partner organisations operating on behalf of the council;
- Employees working at home, from home or remotely;
- Elected members whilst working on council business.

This policy does not apply to those schools with delegated powers, unless adopted by the governing body.

4. Legal Framework

The council must comply with all relevant statutory UK and European Union legislation, including the following that have links to Records Management:

- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Common law duty of confidence
- Copyright, Designs and Patents Act 1988
- Regulation of Investigatory Powers Act 2000
- Health & Social Care Act 2001
- Children Act 2004
- Equality Act 2010
- Re-use of Public Sector Information Regulations 2005
- Criminal Justice and Immigration Act 2008
- Crime and Disorder Act 1998.
- Health and Safety at Work Act 1974.
- Sex Discrimination Acts 1975 and 1986.
- Race Relation Act 1976.
- Limitations Act 1980.
- Companies Acts 1985 and 1989.
- Financial Services Act 1986.
- Value Added Tax Act 1994.
- Civil Evidence Act 1995.
- Electronic Communications Act 2000

More information can be found in appendix C.

5. Linkages with other policies and procedures

This policy is supported by other policies, standards and procedures. These include but are not limited to the following:

- Information Governance Framework Policy
- Freedom of Information Policy
- Environmental Information Regulations Policy
- Data Protection Act Policy
- Information Request Complaints Policy
- Data Breach Policy
- CCTV Code of Practice
- Human resources policies and procedures:
  - Recruitment
  - Employee induction
  - Disciplinary policy
  - Home working, lone working, remote working
- The Finance Manual
- The Humber Information Sharing Charter
- Government Protective Marking Scheme (to be implemented in 2013-14)

6. Definition of Terms Used in Records Management

See appendix A for a list of the definitions of terms used in relation to Records Management.

7. Freedom of Information Act, Environmental Information Regulations and Data Protection Act

Good records management will enable compliance with requests for information under the Freedom of Information Act, Environmental Information Regulations and Data Protection Act. The production of the council's Publication Scheme is also dependent on records being properly managed and this again will ensure compliance with the Freedom of Information Act.

The Data Protection Act in principal five states that information should not be kept for longer than necessary and principal seven states that information must be kept secure. Correct records management will enable compliance.

8. What is a Record?

In the following sections of this policy requirements for the management of records are set out. It is important, to make a distinction between what is and is not a record.

According to the ISO 15489 standard for the management of records, a record is:

> *"Information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business."*

Essentially, it is a record of the council's business that requires effective management and preservation. Records exist in various formats, sometimes with older documents existing in different formats to those created today.

Examples of records include:

- Correspondence.
- Payroll documents.
- Case files.

A non-record, by definition, is an item of information that does not require the same rigour of management that is required for records. A non-record is information that is of immediate value only. Non-records may share some characteristics with administrative records but they are distinguished from administrative records by their transitory usefulness.

Examples of non-records include:

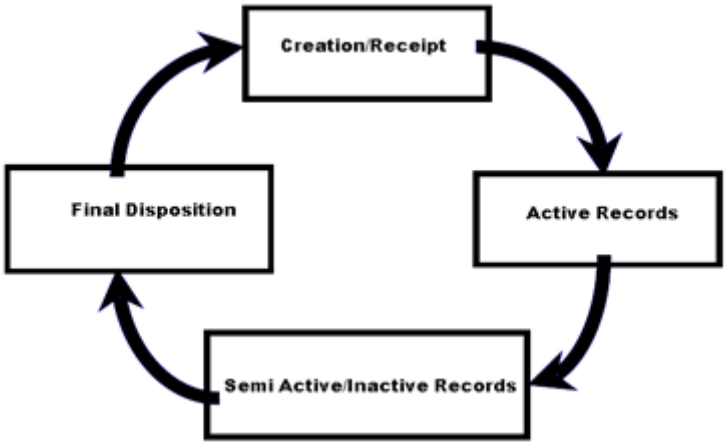
- Reading file copies of correspondence;
- Duplicate copies of original master records, official copies of which have been retained for record purposes;
- Superseded copies of published manuals, policies and directives;
- Catalogues, trade journals, magazines, etc;
- Information copies of correspondence;
- Physical exhibits, artefacts, and material objects lacking documentary values.

Non-records will be disposed of once they have served their useful purpose.

9. Records Management Lifecycle

All information goes through a lifecycle, from its creation to its disposal. At all stages of this lifecycle, processes are used to ensure that its value to the organisation is maximised and that it meets all relevant compliance requirements. Disposal will be in line with the Information and Records Management Society (IRMS) Retention and Disposal Schedule. In addition the council has a retention and disposal schedule for financial documents in the Finance Manual and will work towards creating its own Schedule based on the IRMS guidance.

See below for an example of a typical information lifecycle and explanatory notes:



- **Pre creation** – deciding which information needs to be captured as a record and how.
- **Create/ capture** – information can enter the organisation in many ways. Some is created within; some is derived externally.
- **Index/classify** – the application of descriptive data to records to improve subsequent retrieval and to determine for how long the record should be kept.
- **Store/manage (Active Records)** – records, whether electronic or physical need to be stored and in a way that preserves security, integrity and authenticity and so that they can be accessed efficiently by those authorised to do so.

  Active records are those requiring frequent use and they should generally be stored electronically in an EDRMS, electronically on a shared network drive or within offices if in paper format.
- **Process** – records may need to be processed in order to achieve business aims.
- **Retrieve/disseminate** – to enable the finding of stored records by those who are entitled to search for them.

- **Archive (Inactive Records)** – records that are no longer considered to be 'active' will be sent for either electronic or physical archival storage. This will happen at the point the record is considered to be inactive in that it still required by the council but not for current operational reasons.
- **Destroy or Preserve** – if active records are not required for archive and have outlived any business or statutory requirement to retain further, they may be destroyed or moved for permanent preservation. Archived inactive records reaching their disposal date should also go through the same process.

10. Record Management

Records will be managed to an agreed set of corporate standards, as follows:

Record Creation

Each service area must have in place a record keeping system (paper or electronic) that documents its activities and provides for quick and easy retrieval of information. It must also take into account the legal and regulatory environment specific to the area of work. This system will include:

- Classifying and indexing records in such a way that they can be retrieved quickly and efficiently. The council will develop a corporate classification scheme for organising records.
- Procedures and guidelines for adding the following to all records - referencing, titling, naming conventions, page numbering, dating, authentication and version control, security marking, name of creator, creation date, storage location, method of access and who is permitted access.
- Producing an inventory of 'active' records held so that it is known what records are held, in what format, where, why, for how long they will be kept and if/when they will move into the archives or for permanent preservation. The inventory will also show if there are any duplicate copies of the record.
- Producing an inventory of 'inactive' archived records held so that it is known what records are held, in what format, where, why, for how long they will be kept and when they should be considered for disposal.
- Procedures for keeping the record keeping system updated.
- The ability to cross reference electronic and paper records.
- The creation of backups of electronic records to ensure continuity in the event of record loss or destruction.

Record maintenance and storage

The record keeping system must be maintained so that the records are properly stored and protected, and can easily be located and retrieved. This will include:

- Ensuring that adequate physical or electronic storage space is provided for active records in a dedicated, secure records store or secure electronic system or other electronic storage space.
- Monitoring the movement and location of records so that they can be easily retrieved and provide an audit trail.
- Controlling access to the information.
- Ensuring authenticity so that records retain their legal integrity. In particular, compliance with BS BIP 0008 for legal admissibility.
- Consideration for the provision of the preservation of digital material to allow future access;
- Identifying vital records and applying the appropriate protection, including a recovery plan that ensures the restoration of the business function.
- Ensuring that active records no longer required for the conduct of current business, are identified and transferred to designated archive storage or disposed of in line with the IRMS or other corporate Retention and Disposal Standards.
- Ensuring that inactive records reaching their disposal date are reviewed in line with IRMS or other corporate Retention and Disposal Standards and either retained, passed to a place of permanent preservation or disposed of.

Security and Access

The council recognises the need for consistent and appropriate information to be available in ways that suit the customer and allow the council to function. Providing this availability requires controls that safeguard records and therefore information, including:

- Procedures are in place to document decisions concerning access within the Corporate Classification Scheme.
- All employees are aware of the arrangements for allowing access to certain types of information.
- Records of access to information are kept.
- Accessibility of records should be checked annually to ensure that they remain available or to determine if availability if no longer required and records migrated if necessary.

Retention and disposal

The council will develop and maintain a corporate Retention and Disposal schedule for the retention, archiving and disposal of records to establish the minimum time records should be kept for. This will be based on the IRMS Retention and Disposal Standards. See appendix B for the format of the North Lincolnshire Council schedule.

Prior to completion of the corporate schedule the IRMS retention and disposal standards will be used.

Retention guidelines and schedules relating to financial documents are held in the Finance Manual.

Retention periods will be cross-referenced to the council's Classification Scheme and apply to all records, regardless of form. All records will be disposed of in accordance with the retention schedule. Any errors in the scheme should be highlighted to the Information Management Team immediately. Any records being considered for disposal outside of the disposal date should be discussed with the Information Management Team prior to destruction.

We will also state in the Retention and Disposal Schedule whether the retention period is based on legislation or common practice, where there are no legislation requirements. If common practice is assigned we will assign a 'local rule' retention period to the classification based on the business need and risk.

Retention periods specify the minimum time a record should be kept and what action should be taken at the end of that period. The disposal period will commence from a trigger event (such as the closure of a file).

The disposal of records does not always mean they should be destroyed. In some cases they may be retained longer or transferred to permanent archive. When the disposal date is reached a review will take place to determine whether the record should be destroyed, moved to permanent archive or retained in general archives. This will be based on the risk of destroying the record against its likely usefulness.

Disposition is necessary to comply with the Data Protection Act 1998, principal five that requires records to only kept for as long as necessary. It is also required for the efficient administration of council records, keeping physical or electronic storage to a minimum and not hindering access to information that is still required, such as to respond to Freedom of Information and Environmental Information Regulation Requests.

The retention and disposal process aims to ensure that:

- An intended disposal/review date is captured when creating records in all forms. This will be based upon the classification of records and the retention and disposal schedule.
- Retained records are reviewed each year in accordance with the Retention Schedule and those records reaching the disposal date are considered for disposal.
- When records reach the disposal date the relevant inventory will be updated to reflect the action taken.
- Disposal of records documentation will be completed and retained whenever a record is disposed of. This may be necessary to provide evidence that a record is no longer held, for example in response to a Freedom of Information request. Destruction Form IG01 should be used.
- If records are transferred for permanent preservation transfer of records documentation will be completed and retained. Transfer Form IG02 should be used.
- Records subject to an outstanding request for information or legal proceedings will not be destroyed until after the request has been answered and/or the legal proceedings are completed.
- Destruction of redundant material will be carried out in accordance with its level of sensitivity and in line with the Information Security Policy.

11. Classification Scheme

A classification scheme is a way of organising records to make the management of them easier. These schemes are almost invariably hierarchical in structure with classes that represent broad “functions” sub-divided into more detailed sub-classes.

There are five main reasons for classifying information:

1. Documents of a similar theme are kept together and placed into context. A single record supplies a limited amount of information. A group of related records (perhaps maintenance records for a property) provides much more information.
2. It helps to find information. The classification can act as a guide to locating information on a particular topic.
3. It allows access controls to be applied. Applying controls to every individual document is impossibly time-consuming. Applying controls to information with the same classification reduces the administration to manageable levels.

4. It allows retention schedules to be applied and provides a basis for storing information. Like access controls, applying retention schedules to individual documents would not be practical.
5. It allows ownership and management responsibility to be attached to groups of records, which again would not be as easy for individual records.

North Lincolnshire Council Classification Scheme

The council will develop a corporate Classification Scheme to be used as the basis for storing documents and records and applying access controls and retention schedules.

The scheme will be based on the Local Government Classification Scheme (LGCS), but tailored to meet the council's specific corporate requirements. The scheme will be based on functions carried out by the council.

The corporate Classification Scheme will include all records regardless of format such as:

1. Physical records including documents, but also other physical records such as microfilm;
2. Networked file storage;
3. Emails;
4. Business application systems.

In the case of business application systems, the classification scheme may incorporate the existing structure of the information. Typically, such information is stored under a unique identifier, either a person (such as a benefit claimant) or a physical structure (such as a property).

12. Management of electronic records

The principal issues for the management of electronic records are the same as those for the management of any record. However, the means by which these issues are addressed in the electronic environment will be different.

Effective electronic record keeping requires:

- A clear understanding of the nature of electronic records;
- The creation of records and metadata necessary to document business processes: this should be part of the systems which hold the records;
- The maintenance of a structure of folders to reflect logical groupings of records;
- The secure maintenance of the integrity of electronic records to help prevent accidental or unauthorised alteration, copying, moving or deletion;
- The accessibility and use of electronic records for as long as required (which may include their migration across systems);

- The application of appropriate disposal procedures, including procedures for archiving;
- The ability to cross reference electronic records to their paper counterparts in a mixed environment.
- The ability to retain and dispose of emails in line with this policy. These guidelines will be developed.

Audit trails should be provided for all electronic information and documents. They should be kept securely and be available for inspection by authorised personnel.

13. Roles and Responsibilities

Full details of the council's Information Governance roles and responsibilities are set out in the Information Governance Policy Framework. The following roles and responsibilities have specific involvement with Records Management:

Principal Information Governance Officer (Data Protection Officer & Deputy SIRO)

The Principal Information Governance Officer is responsible for:

- Creating a Records Management process which complies with relevant legislation;
- Promoting compliance with this policy;
- Providing expert advice to Records Co-ordinators and other council employees on compliance with this policy;
- Investigating non compliance with this policy.

Democratic & Legal Services are responsible for providing legal advice in respect of relevant legislation.

Records Co-ordinators

Each directorate/service is assigned a Records Co-ordinator and it is their responsibility, over and above those responsibilities assigned to all employees, to:

- Ensure records are managed in line with this policy;
- Assist managers with compliance with this policy and therefore relevant legislation;
- Work in conjunction with information request co-ordinators and Legal Services to ensure records are retained past the minimum disposal date when necessary;
- Make decisions in conjunction with Information Management about Common Practice Retention rules;

- Ensure along with the Information Asset owner that records are disposed of or retained in line with this policy;
- Report any breaches or potential breaches of this policy to the Senior Information Risk Owner (SIRO) or Principal Information Governance Officer.

14. Audit

Records Management policy, standards and procedures will be audited periodically as part of the annual internal audit work plan, to ensure compliance.

15. Monitoring and Review

The current version of this policy can be found on intralinc and the council website along with information supporting this policy. This policy and all supporting procedures will be reviewed as it is deemed appropriate but no less frequently than every 12 months.

Appendix A – Key Records Management Definitions

Term	Definition
Classification	Identification and arrangement of business activities and/or records into categories according in this instance to function.
Destruction	Process of deleting or destroying records, beyond any possible reconstruction.
Disposition	Range of processes associated with implementing records retention, destruction or transfer decisions.
Document	Recorded information or object, which can be treated as a unit.
Indexing	Process of a process to facilitate retrieval of records and/or information.
Metadata	Data describing context, content and structure of records and their management through time.
Preservation	Processes and operations involved in ensuring the technical and intellectual survival of records through time.
Records	Information created, received, and maintained as evidence and information by an organisation or person, to fulfil legal obligations or business requirements.
Records system	Information system, which captures, manages and provides access to records through time.
Tracking	Creating, capturing and maintaining information about the movement and use of records
Transfer	Change of ownership and/or responsibility for records or moving records from one location to another.

Appendix B – Retention & Disposal Format

Classification / PMS Classification	Record Description	Information Asset Owner	Format of Record	Location of Record	Minimum Retention	Legislation / Common Practice	Retention Trigger	Review Action

Key:

Classification / PMS Classification
Classification grouping and protective marking applied to the group of records.

Record Description
Description of the record.

Information Asset Owner
The owner of the group of records.

Format of Record
Whether the record is in paper, electronic or other format.

Location of Record
Where the record is stored either physically if in paper format or in which system or electronic storage area if electronic.

Minimum Retention
The minimum time the record must be retained for.

Legislation / Common Practice
The legal or business reason for the retention of the records.

Retention Trigger
The event which indicates when the retention period begins.

Review Action
The action that should be taken when a review is carried out at the point the record reaches its minimum retention date.

Appendix C – Standards and Compliance

Data Protection Act 1998
Principals setting out how the council must deal with personal information and the right for individuals to gain access to the personal data that is held about them.

Freedom of Information Act 2000
Public access rights to all information held by a public authority, other than that which is exempt.

Environmental Information Regulations 2002
Public access rights to environmental information.

Local Government Act 1972
Section 224 of the Act requires local authorities to make proper arrangements in respect of the records they create.

Public Records Acts of 1958 and 1967
All public bodies have a statutory obligation to keep records in accordance with the Public Records Act. This places the responsibility on government departments and other organisations within the scope of the Act for making arrangements for selecting those of their records, which ought to be permanently preserved, and for keeping them in proper conditions. Parts of this Act have been superseded – particularly by the FOIA.

Limitation Act 1980
Has particular relevance to applying appropriate retention periods. For example, in regard to financial records, the Act "provides that an action to recover any sum recoverable by any enactment shall not be brought after the expiration of six years from the date on which the cause of the action accrued".

Health and Safety at Work Act 1974
Influences how long records relating to Health and Safety incidents should be retained.

Human Rights Act 1998
Particular relevance in relation to an individual's right to privacy.

Regulation of Investigatory Powers Act, 2000
Deals with the interception of communications and governs what government bodies can do and what limits apply. Organisations must be able to show, through auditing, that authorised personnel only access their data.

International standard for records management: ISO 15489
Aims to ensure that appropriate attention and protection is given to all records, and that the evidence and information they contain can be retrieved more efficiently and effectively, using standard practices and procedures.

Code of practice for information security management: ISO 17799
ISO 17799 describes a structured set of control objectives, the implementation of which is guided by an assessment of information security risks. It also proposes a governance framework for the management and implementation of information security.

Information Security Management System requirements: ISO 27001
This is complementary to ISO 17799 and defines the requirements for an Information Security Management System (ISMS). This, effectively, describes the process for creating an ISMS, implementing and managing the governance and controls described in ISO 17799.

Code of practice for Legal Admissibility: BIP 0008
Provides a framework and code of good practice for the implementation and operation of information storage systems, whether or not any information held therein is ever required as evidence in event of a dispute.

e-Government Interoperability Framework: e-GIF
e-GIF defines the technical policies and specifications governing information flows across government and the public sector. They cover interconnectivity, data integration, e-services access and content management.

e-Government Metadata Standard: e-GMS
e-GMS is a subset of the e-GIF and lays down the elements, refinements and encoding schemes to be used by government officers when creating metadata for their information resources or when designing search systems for information systems.

Local Government Classification Scheme
This scheme seeks to achieve control over both electronic and physical records by ensuring that records, whatever their medium, are stored consistently. It aims to achieve this by ensuring that records be logically stored together and thereby "facilitate and enhance the capacity of the organisation to share information".

Retention Guidelines for Local Authorities - Records Management Society
Guidance for local authorities on the retention and disposal of common functional and housekeeping records. To be used as a baseline to interpret and apply appropriately in accordance with local practice.

Building Systems Fit for Audit: BSI PD 0018
To ensure that information systems can easily be audited.

Lord Chancellor's Code of Practice on the Management of Records, Issued under section 46 of the FOIA
This Code of Practice gives guidance on good practice in records management.

The National Archives' Requirements for Electronic Records Management Systems

Requirements used by TNA's system evaluation programme. Many of the leading systems have been formally assessed and approved against these requirements.

Model Requirements for the Management of Electronic Records: MoReq

Requirements specifications funded by the European Commission. The second version of these requirements, MOREQ2 supersede the TNA requirements as being the principal standard by which such systems are judged.

North Lincolnshire Council

Freedom of Information, Environmental Information Regulation & Data Protection Customer Complaints Policy

1. Introduction

North Lincolnshire Council is committed to delivering excellent customer service. Listening to our customers and learning from customer feedback enables the council to improve its services and meet the needs of customers more effectively.

We want to make it as easy as possible for customers to let us know their views, including how to make a complaint.

This policy sets out how customers can make a complaint about: -

- requests for information under Freedom of Information (FOI) Act or Environmental Information Regulations (EIR)
- requests for personal information under the Data Protection (DP) Act
- the way in which personal data has been handled in relation to the Data Protection (DP) Act

and how we will respond to and learn from complaints received.

2. Our Customers

This policy applies to any customer of the council, or a person or body acting on behalf of the customer who has a complaint about FOI, EIR or DP as detailed in section 1.

In this instance a customer of the council is anyone who: -

- contacts the council to seek information using the FOI, EIR or DP processes
- contacts the council to report a concern about how personal information is being handled.

3. Complaints

Definition of an FOI, EIR or DP Complaint

An FOI, EIR or DP complaint is any expression of dissatisfaction about the council's handling of your request for information, or standard and quality of service in relation to FOI, EIR or DP – which requires a response. The response may be to put things right straightaway, or to investigate the matter further.

A complaint could include any of the following concerns:

- we **delay** or **fail to deliver** a request for information
- we **fail** to resolve a request to handle your personal information as we should
- a member of staff's **attitude** or **competence** causes concern
- we **fail to meet** our statutory responsibilities in relation to FOI, EIR or DP
- we **apply** an exemption that you are not happy about.

A complaint **is not:**

- a first request for service
- a query about progress of a specific issue

4. FOI, EIR & DP Complaints Procedure

Customers must make a formal FOI, EIR or DP complaint about the council in writing online, by email or by post. If assistance is required to put a complaint into writing the complaint can be made in person via a Local Link.

Informal complaints can be made in writing but can also be made via the telephone.

See Appendix 1 for ways to contact the council.

Informal Resolution

Where the FOI, EIR or DP complaint is of a general nature we aim to resolve the issue informally.

We encourage customers in this first instance to contact the FOI/EIR or DP Co-ordinator of the service they wish to complain about. The Co-ordinator will do all they can to put things right.

Formal Resolution

Where the FOI, EIR or DP complaint is related to a perceived breach of the FOI or DP Acts or the EIR Regulations the complaint will be investigated through the council's formal procedure. The formal complaint process will be carried out as a one stage internal review.

Please note – EIR complaints must be made within 40 working days of the alleged failure to apply the regulations.

Formal Process
A service FOI/EIR or DP Co-ordinator will ensure an appropriate service manager carries out the internal review of the complaint along with the Head of Information Management.

An acknowledgement will be sent to the customer within 5 working days and a response will be sent within 20 working days. This timescale for the sending of the response can be extended to within 40 working days for in depth internal reviews. The complainant will be informed about this extension and the reason for it.

How to appeal against the outcome of a FOI, EIR or DP complaint

Where the council has internally reviewed a FOI, EIR or DP complaint and the customer is still not satisfied, they may appeal to the Information Commissioner (see Appendix 1 for contact details).

For FOI and EIR complaints the appeal must be made to the Information Commissioner within 6 months of the outcome of the internal review.

5. Responding to FOI, EIR or DP Complaints

On receipt of a formal FOI, EIR or DP complaint we will:

- ensure it is recorded on the council's system for tracking complaints
- ensure it is forwarded to the appropriate FOI, EIR or DP Co-ordinator for action.

We will acknowledge and respond to the complaint or send a holding letter to the customer in line with the timescales indicated in section 4.

We will at all times deal with FOI, EIR or DP complaints courteously, openly and fairly.

FOI, EIR or DP Complaints – Upheld

Where we have made a mistake or failed to provide the expected standard or quality of service, we will acknowledge and apologise for this. We will also set out the actions we will take to put things right and improve our services. This could include:

- Providing previously withheld information
- reviewing council FOI, EIR or DP policies or procedures
- reviewing how we handle personal data
- providing appropriate staff training and guidance

FOI, EIR or DP Complaints – Not Upheld

Where we have investigated and we still up hold the original decision we made, we will:

- explain the reasons for our decision clearly
- provide any relevant evidence to support the decision
- inform customers how to progress their complaint if they remain dissatisfied.

6. Persistent and Vexatious FOI, EIR or DP Complaints

We aim to respond to all FOI, EIR & DP complaints positively, and ensure that customers are satisfied with the way their complaint has been handled.

In a small number of cases customers may pursue a complaint in an unreasonable way, which impacts, on council resources and capacity to respond to the complaint effectively.

Ways in which a customer may be considered unreasonably persistent or vexatious in pursuing their FOI, EIR or DP complaint could include:

- changing the basis of a complaint during the investigation process
- refusing to co-operate with the complaints investigation process
- refusing to accept investigation conclusions and decisions
- repeatedly making the same or similar complaint

Continuing to respond to these complaints can take up a lot of time and reduce capacity to deal with other complaints effectively.

Where an officer considers that a FOI, EIR or DP complaint has become vexatious, the matter will be referred to the Head of Information Management. The Head of Information Management will seek legal advice and decide whether to pursue the complaint any further. If applicable, the Head of Information Management will inform the customer that the complaint has been closed and that the council will not enter into any further correspondence on the matter.

7. Learning from FOI, EIR & DP complaints

We collect and review feedback from our customers, and use this information to drive service improvement.

All FOI, EIR & DP complaints are recorded on the council's tracking system. Data about complaints is collated and shared across the council to identify performance trends and review how we handle and respond to customer feedback. This includes:

- how well we meet our target response times
- how effective we are in capturing complaints across the council

FOI, EIR & DP complaints are regularly reviewed across the council to identify how we can improve our FOI, EIR or DP processes. This includes:

- service managers or the Head of Information Management making operational improvements in response to specific complaints
- regular review of upheld complaints at directorate and corporate performance reviews to identify issues that need addressing
- development action plans to improve services based on specific issues or trends in complaints

The council will publish information about FOI, EIR & DP complaints – to inform customers about how we handle complaints and show how we make changes as a result of customer feedback.

8. Confidentiality

Any personal data provided to the council will be managed in line with the requirements of the Data Protection Act 1988. The council will use this information to respond to the customer and improve services.

Personal data will be kept anonymous in producing and sharing information about FOI, EIR or DP complaints with other services and partners.

Appendix 1 - Contact Information

How to contact the council

Telephone – informal complaints only
01724 297000

Website
On the council's website by clicking the 'Contact Us' link on the home page:
www.northlincs.gov.uk

Email
By email to customerservice@northlincs.gov.uk

Post
In writing to 'Customer Feedback' FREEPOST NEA 10154, Civic Centre, Ashby Road, Scunthorpe DN16 1AB

In Person
By contacting one of our advisors at a Local Link Office – listed below

Local Link Offices
Ashby Library & Local Link - Ashby High Street, Scunthorpe, DN16 2RY
Barton Local Link - Providence House, Holydyke, Barton, DN18 5PR
Brigg & District Local Link - Hewson House, Station Road, Brigg, DN20 8XB

Crowle Community Hub - 52 – 54 High Street, Crowle, DN17 4DR

Epworth Library & Local Link - Chapel Street, Epworth, DN9 1HQ

Scunthorpe Local Link - Church Square House, 30 – 40 High Street, Scunthorpe, DN15 6NL

Winterton Library & Resource Centre - West Street, Winterton, DN15 9QJ

Information Commissioner

Address: Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF; Telephone: 0303 123 1113 or 01652 545700; email: notification@ico.gsi.gov.uk; Web: www.ico.gov.uk

Data Protection Act Policy

www.northlincs.gov.uk

Document History

Purpose	
Document Purpose	To provide a corporate policy for the Data Protection Act
Document developed by	Head of Information Management
Document Location	This document is located on the council's web site and on the network at: *C:\DOCUME~1\CHRISD~2\LOCALS~1\Temp\Domino Web Access\IM Policy Refresh March13 v2.1.doc*

Revision	
Revision date	**07 March 2013**
Version	Draft v.1.2
Status	Draft awaiting approval
Summary of changes	Completely revised in line with the NHS's Information Governance framework requirements.

Approvals	
Head of Information Management	Lead the review of the framework and policies
Assistant Director, Business Support	Oversee the document through the council's approval process
Improvement & VFM Group	Approve the Framework and the Data Protection Act Policy and any changes made, recommending adoption to CMT
Cabinet	Approve the review of the framework and policies

Contents Page

1. Introduction

The Data Protection Act 1998 (Act) implements the European Data Protection Directive in the UK and it came into force on 1st March 2000. The Information Commissioner's Office (ICO) regulates the Data Protection Act in the UK and a copy of their guidance note about this legislation can be accessed at www.ico.gov.uk.

The Data Protection Act applies to personal information processed by an organisation. To operate efficiently the council has to collect and use information about individuals with whom it works. These may include members of the public, current, past and prospective employees, clients and customers, and suppliers. In addition, it may be required by law to collect and use information to comply with the requirements of central government. Personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means. There are safeguards to ensure this in the Data Protection Act.

This policy outlines the principles of the Data Protection Act and the rights given to individuals, how the council will comply with these and the responsibilities assigned to key employees. In addition it outlines our requirement to notify the Information Commissioner as to when we process personal information. Also outlined are our procedures that aim to ensure all employees, elected members, contractors, agents, consultants, partners or other servants of the council who have access to any personal data held by or on behalf of the council, are fully aware of and abide by their duties and responsibilities under the Data Protection Act.

The council regards the lawful and correct treatment of personal information as very important to successful operations and to maintaining confidence between those with whom we deal and ourselves. It ensures that personal information is treated lawfully and correctly, protecting the rights and freedoms of individuals with respect to the processing of their personal information. To this end, the council fully endorses and adheres to the Principles of Data Protection as set out in the Act.

The council is the Data Controller for personal information it holds or is held on its behalf, and could be liable as an organisation for any breaches of this policy. This could result in the issue of a monetary penalty of up to £500,000 by the Information Commissioner or other legal action. Liability could extend to individual employees in certain circumstances, such as if personal information were to be unlawfully obtained or disclosed. Anyone permitted to access our personal information must comply with this policy. Any breaches of this policy will be investigated and could result in action being taken under the Disciplinary Policy.

All requests for information are recorded in a single corporate register with a unique identification reference number. They are managed using the Council's Firmstep Customer Relationship Management (CRM) system.

This policy is part of a suite of information governance policies.

2. Purpose

The purpose of this policy is to ensure compliance with the Data Protection Act when the council processes personal information. This will be achieved by ensuring that personal information is processed as set out in this policy and in the council's notification to the Information Commissioner and therefore as required by the Data Protection Act.

3. Scope

This policy applies to all personal information held by the council or held on behalf of the council. This includes information on paper and in electronic formats, including personal information collected by the council's CCTV cameras.

The scope of this policy extends to:

- Employees and others, including contractors, volunteers, agencies and partner organisations operating on behalf of the council, who have access to personal information.;
- Elected members whilst working on council business.
  (Elected members are separate data controllers when carrying out electoral ward duties – these responsibilities are not covered by this policy. Schools are also separate Data Controllers);
- The policy includes employees working at home, from home or remotely.

This policy does not apply to those schools with delegated powers, unless adopted by the governing body.

4. Legal Framework

The council must comply with all relevant statutory UK and European Union legislation, including the following that have links to the Data Protection Act:

- Human Rights Act 1998
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Common law duty of confidence
- Copyright, Designs and Patents Act 1988
- Regulation of Investigatory Powers Act 2000

- Health & Social Care Act 2001
- Children Act 2004
- Equality Act 2010
- Criminal Justice and Immigration Act 2008
- Crime and Disorder Act 1998.

5. Linkages with other policies and procedures

This policy is supported by other policies, standards and procedures. These include but are not limited to the following:

- Information Governance Framework Policy
- Freedom of Information Policy
- Environmental Information Regulations Policy
- Records Management Policy
- Information Sharing Policy
- Data Quality Policy
- Information Request Charging Policy
- Information Complaints Policy
- Data Breach Policy
- CCTV Policy
- Human resources policies and procedures:
    - Recruitment
    - Employee induction
    - Disciplinary policy
    - Home working, lone working, remote working
- Employee Code of Conduct
- The Humber Information Sharing Charter

6. Definition of Terms Used in the Data Protection Act

See appendix A for a list of the definitions of terms used in the Data Protection Act.

7. When does the Data Protection Act Apply?

In the Data Protection Act 1998 data means:

1. Information that is processed automatically
2. Information that is recorded with the intention that it should be processed automatically
3. Information that is recorded as part of a relevant filing system or with the intention of being part of such as system.

4. Information that does not fall within the above three categories but which forms part of an accessible record. Records considered to be accessible include health records, educational records (local education authority and special schools only), local authority housing records and local authority social service records.
5. Information which is recorded and held by a public authority which does not fall within the above four categories.

This means that the handling (processing) of any personal information obtained about an individual (data subject), which is or could be used by the council, is covered by the Data Protection Act from the time it is collected through its recording, retrieving, disclosure and destruction. It could be information collected on paper, recorded in a computer, or recorded on other material, such as from a taped interview or a CCTV image.

However, to be considered personal information and therefore covered by the Data Protection Act the information must be about a living individual, who can be identified directly from the information or from additional information, which is in (or likely to come into) the possession of that individual.

A 'relevant filing system' is one where information is organised either by reference to individuals or by criteria relating to individuals so that a specific detail about a person may be easily selected from the system.

8. Principals of the Data Protection Act

The council has a duty under the Data Protection Act, unless an exemption applies, to comply with eight legally enforceable principles, as summarised below.

Personal information should be:

1. Fairly and lawfully processed;
2. Obtained for specified purposes and not used for other incompatible purposes;
3. Adequate, relevant and not excessive;
4. Accurate and up to date;
5. Not kept for longer than necessary;
6. Processed in line with the rights of individuals;
7. Kept secure;
8. Not transferred to countries outside of the European Economic Area unless adequate protection is assured.

9. Rights of Individuals

The Data Protection Act 1998 allows individuals to:

1. Request a copy of the personal information held about them by an organisation. These requests are known by the Act as 'Subject Access Requests' or 'SARs'.

Following is a summary of this process. Further information is available on the Information Commissioner's website at www.ico.gov.uk.

Requests for personal information:

- Must be in writing.
- Must provide enough information to determine the information required.
- Must be accompanied by the £10 fee we are permitted to charge. (If the information is from an Official School Record the charge is based on a sliding scale from £1 to £50 dependent on the number of pages)
- Must be accompanied by identification to help prevent fraudulent requests for information, unless we can satisfactorily identify the data subject without identification.
- Can be made via a 3rd party, such as a solicitor or someone holding power of attorney, with the permission of the data subject.

The council may be entitled to refuse any requests on procedural grounds, such as when the above points are not complied with.

If we are able to release the requested information we will collate it, advise the requester of the source of this information and provide a permanent copy. Sometimes an exemption will prevent us from releasing the information. Where information can be released we aim to provide it within 40 consecutive days (15 school days for Official Education Record information).

If a request for information that should be handled under another information request regime or as a combination of regimes the requester will be advised. An example is when a request for non personal information is made under the Protection Act. In this instance the request would be considered under the Freedom of Information Act.

If the information cannot be released within this time period there must be a valid reason for the delay and the data subject will be kept informed of progress and given access to any personal information as it becomes available. The information provided will be in permanent form, such as a written document, unless we are unable to provide a permanent copy.

If we are unable to provide some or all of the requested information because, for example this information is exempt from disclosure, we will explain in writing within 40 consecutive days.

Generally the only fee or charge, which applies to a subject access request, is the statutory fee, mentioned above. However, if the request is for third party personal information or if the requested information is located in an unstructured manual filing system the request may be dealt with under the Freedom of Information Act 2000. In this instance the Freedom of Information and Data Protection (Appropriate Limit and Fees) Regulations apply and there may be other charges. Please see the policy about these fees on our website www.northlincs.gov.uk for more information.

We will provide advice with each request about how to make a complaint, and how to appeal to the ICO should be requester be unhappy with how we have handled the request for information.

2. Request that inaccurate information is rectified, erased, destroyed or blocked.

Individuals can ask that inaccurate personal information is corrected or deleted.

3. Prevention of processing likely to cause damage or distress.

Individuals can ask that the handling of their personal information be stopped if it is causing or is likely to cause substantial damage or distress to the individual or another person.

4. Prevention of processing for direct marketing.

Individuals can ask that their personal information is not used or is no longer used for direct marketing.

5. Rights in relation to automated decision taking.

Individuals have the right to prevent decisions, which significantly affect them; being based just on processing by automated means.

6. Right to compensation.

An individual, who suffers damage or distress as a result of a contravention of the Data Protection Act principals by a Data Controller, is entitled to claim compensation. This only applies if the Data Controller is unable to demonstrate that reasonable care was taken to comply with the principal.

When responding to the rights of an individual as set out in 2. to 6. we will do so in writing explaining any action we have taken or are unable to take. We will also provide advice with each response about how to make a complaint, should be individual be unhappy with how we have handled their concern.

10. Contact Details

All requests should be made in writing to Customer Services using the following contact details:

Website
Via the council's website by clicking the 'Contact Us' link on the home page: www.northlincs.gov.uk

Email
By email to inforequest@northlincs.gov.uk

Post
By writing to 'North Lincolnshire Council, Customer Services, Church Square House, 30-40 High Street, Scunthorpe DN15 6NL

Assistance Required
If you need help to make a request or to put your request in writing please contact one of our advisors at a Local Link Office – see the council's website or appendix B for Local Link details.

11. Compliance with the Data Protection Act

The council will, through appropriate management, strict criteria and controls ensure that all employees and other individuals with access to personal information comply with this policy and accept personal responsibility for doing so by:

1. Observing fully conditions regarding the fair and lawful collection of and use of personal information.
2. Meeting our legal obligations for specifying the purpose for which personal information is collected and used;
3. Collecting and processing appropriate information only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements.
4. Ensuring the quality of personal information created, used and held;
5. Keeping all personal information secure;
6. Applying strict checks to determine the length of time personal information should be held and ensuring it is not kept for longer than is necessary;
7. Ensuring that individuals are aware of their rights under the Act and that they are able to exercise them. These include being able to request a copy of personal information held;
8. Only applying exemptions as permitted by the Act.

9. Ensuring that any third party processors contracted by the Council adhere to appropriate controls;
10. Only transferring personal information outside of the European Economic Area (EEA) when assurance is given that it will be adequately protected;
11. Investigating and responding to complaints in relation to the Act as set out in the Information Request Complaints Policy.

12. Notification to the Information Commissioner

The Data Protection Act requires that the council, as a processor of personal information, registers each year with the Information Commissioner. This registration is known as notification and it details when the council is processing personal information under a series of 'purposes'.

The North Lincolnshire Council registration number is Z563337X and full details of this document can be viewed on the ICO website using the following link www.ico.gov.uk.

We will ensure that this registration is made each year and that it is reviewed annually, prior to renewal.

13. Privacy Notice

The council will ensure that individuals are made aware of personal information being held by the council and how this information is being used, held, who can access it, with whom it is being shared and for how long it will be kept. This will be by Privacy Notices and will happen where the use of the personal information is not obvious.

There is a general Privacy Notice on the council's website. Additional more specific Privacy Notices will, where applicable, also be clearly stated on written literature, on council web pages and verbally, if individuals are being spoken to face to face or by telephone.

Please note that there are instances, as permitted by the Data Protection Act, when individuals will not be made aware of this information. An example is personal information in connection with the prevention and detection of crime.

14. Roles and Responsibilities

Full details of the council's Information Governance roles and responsibilities are set out in the Information Governance Policy Framework. The following roles and responsibilities are specific to compliance with the Data Protection Act:

Principal Information Governance Officer (Data Protection Officer & Deputy SIRO)

The Principal Information Governance Officer is responsible for:

- Creating a process for handling of requests for personal information and for handling requests in relation to the other rights of individuals;
- Promoting compliance with this policy and therefore the Data Protection Act;
- Providing expert advice to Data Protection Co-ordinators and other council employees on compliance with this policy and the Data Protection Act;
- Completing, submitting and managing notifications to the ICO;
- Leading complaint investigations in relation to the Data Protection Act;
- Carrying out corporate reviews of processes to ensure compliance with the Data Protection Act;
- Investigating non compliance with this policy.

Democratic & Legal Services are responsible for providing legal advice in respect of the Data Protection Act.

Data Protection Co-ordinators

Each directorate/service is assigned a Data Protection Co-ordinator and it is their responsibility to:

- Process requests for personal information;
- Process other requests from individuals in relation to their rights under the Data Protection Act;
- Promote compliance with compliance with this policy and therefore the Data Protection Act;
- Report any breaches or potential breaches of this policy to the Senior Information Risk Owner (SIRO) or Principal Information Governance Officer.

15. Complaints

The Council is determined to ensure that its services are as efficient and effective as possible. If people feel that their request has not been dealt with in a satisfactory manner it will be reviewed using the Council's FOI, DP and EIR Complaints Policy, details of which are located on the website.

Complaints will be investigated and we aim to ensure the complainant receives a response within 20 working days.

Anyone not happy with the outcome or the handling of the council's internal review may seek an independent review from the Information Commissioner and requests should be made in writing to:

The Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF
Telephone: 01625-545700 / Fax: 01625-545510

16. Audit

The Data Protection Act policy, standards and procedures will be audited periodically as part of the annual internal audit work plan, to ensure compliance.

17. Monitoring and Review

The current version of this policy can be found on intralinc and the council website along with information supporting this policy. This policy and all supporting procedures will be reviewed as it is deemed appropriate but no less frequently than every 12 months.

Non compliance with this policy will be investigated by the Information Management Team, in conjunction with HR if disciplinary action may be required. Data Breaches will be investigated as per the council's Data Breach Policy, available on the internet at www.northlincs.gov.uk.

Appendix A – Key Definitions

Data – is defined under the Data Protection Act as:

1. Information that is processed automatically
2. Information that is recorded with the intention that it should be processed automatically
3. Information that is recorded as part of a relevant filing system or with the intention of being part of such as system.
4. Information that does not fall within the above three categories but which forms part of an accessible record. Records considered to be accessible are health records, educational records (local education authority and special schools only), local authority housing records and local authority social service records.
5. Information which is recorded and held by a public authority which does not fall within the above four categories.

Personal Data – is that which relates to a living individual.

Sensitive Personal Data – is information relating to a living individuals race/ethnic origin, religion, sexual life, health, trade union membership, political opinions or criminal/alleged criminal offences.

Data Processing – relates to almost any activity carried out in relation to personal information. Examples are holding the information, releasing it, amending it and destroying it.

Data Controller – The individual or organisation that decides how and why personal information will be processed.

Data Processor – An individual or organisation that process personal information on behalf of the Data Controller, under instruction from the Data Controller.

Data Subject – An individual who is the subject of the personal information.

Appendix B – Local Link Office details

Local Link Offices

Ashby Library & Local Link - Ashby High Street, Scunthorpe, DN16 2RY

Barton Local Link - Providence House, Holydyke, Barton, DN18 5PR

Brigg & District Local Link – The Angel, Market Place, Brigg, DN20 8LD

Crowle Community Hub - 52 – 54 High Street, Crowle, DN17 4DR

Epworth Library & Local Link - Chapel Street, Epworth, DN9 1HQ

Scunthorpe Local Link - Church Square House, 30 – 40 High Street, Scunthorpe, DN15 6NL

Winterton Library & Resource Centre - West Street, Winterton, DN15 9QJ

External Ref:	HIG 01
Review date	March 2013
Version No.	V04
Internal Ref:	NELC 16.60.01

Humber Information Sharing Charter

This Charter may be an uncontrolled copy, please check the source of this document before use. Refer to the 'Strategy and Policy Register' or Humber data observatory website (www.humberdataobservatory.org.uk) for the latest version.

This Charter supersedes all previous versions of this Charter including the Community Charter for Information Sharing (North East and North Lincolnshire) and the General Protocol for Information Sharing between agencies in Kingston upon Hull and the East Riding of Yorkshire.

NORTH EAST LINCOLNSHIRE COUNCIL www.nelincs.gov.uk	Maintenance and control of the Charter is undertaken by North East Lincolnshire Council on behalf of the Humber Information Governance Group, all enquiries should be addressed to transparency@nelincs.gov.uk

Contents

Humber Information Sharing Charter

Appendices

Humber Information Sharing Charter

1. Introduction

1.1 The appropriate exchange of information is essential to deliver effective and efficient services for our citizens, to meet their needs and ensure their welfare and protection. However there is a balance between the need to share sufficient information to deliver effective services, and preserving the privacy of the individual.

1.2 To assist understanding and the application of effective information sharing it is helpful to have locally documented clarity about how legal constraints 'fit' with practice guidelines, identifying what can and cannot be shared with whom, how and for what purposes.

1.3 This Charter provides a framework for the effective and secure sharing of information in accordance with legal requirements, ethical boundaries and good practice across the Humber region. It will ensure transparency of information governance practices, assist the documenting of information sharing decisions and actions to ensure they are auditable, and raise awareness of the legal and ethical boundaries around information disclosure and the rules and methods for accessing data.

1.4 The Charter is based on the Three Tier Model for Information Sharing, which requires that Information Sharing be considered at three levels of complexity; a higher level 'Charter' which establishes the Principles and standards for information sharing; a middle level set of Protocols which agree the Purposes for which information will be shared; and a lower level set of specific agreements which define the processes by which information can and will be shared and with who.

1.5 The Charter does not impose new obligations on signatory organisations, but reflects current regulations and legislation for the sharing of personal information, and builds on existing partnerships.

2. Objectives of the Charter

2.1 The signatories to this Charter recognise the importance of sharing information effectively and securely for the purposes of delivering and improving outcomes for the citizens and communities we serve.

2.2 Through this Charter the signatories aim to achieve consistent and good practice for the sharing of personal information.

- Providing signatory organisations and those acting on their behalf with clear guidelines to follow for the secure and confidential sharing of personal information in accordance with legal requirements.

- Informing citizens why personal information about them may need to be shared between signatory organisations, and how that information will be shared and used.

3 Our commitment

3.1 As a signatory organisation we are committed to ensuring that the identifiable personal information we collect, hold and use will be processed in accordance with legalisation, best practice and the expectations of citizens, to meet and ensure security and confidentiality requirements. This Charter sets out the principles and minimum standards that will underpin the processing and exchange of personal information.

4 Designated Officer

4.1 As a signatory organisation we must have in place a Designated Officer, responsible for approving and monitoring the processing of personal information in accordance with the Humber Information Sharing Charter.

4.2 For Health organisations this will be the Caldicott Guardian, for signatory organisations signed up to Public Service Networks it will be the Senior Information Risk Officer and for Social Care organisations this will be the Caldicott Guardian and the Senior Information Risk Officer. For all other organisations it will be a senior officer with responsibility for information governance nominated by the Chief Executive or equivalent.

5 The principles guiding the sharing of information

5.1 As a signatory organisation we will work to:

A) Support and promote the accurate, timely, secure and confidential sharing of both person identifiable and anonymous information in accordance with our legal, statutory and common law duties, and the requirements of this Charter and other additional guidance as notified to us;

B) Ensure a copy of the Charter and the identity of the Designated Officer are clearly and widely promoted across the organisation and available to all;

C) Have in place effective policies and procedures to meet our responsibilities for the secure and confidential sharing of information, aligned to statutory requirements and this Charter;

D) Ensure that all employees and those acting on our behalf are aware of, understand and comply with their responsibilities for information security and confidentiality through appropriate promotion, training, monitoring and enforcement;

E) Ensure all our data meets the high standards identified in the Audit Commission's "Improving information to support decision making: standards for better quality data", November 2007, and any locally agreed protocols.

5.2 When sharing information we will endeavour to ensure that:

F) Individuals are fully informed about the information held about them and how it will be used and shared;

G) Information will be shared with consent, except where statutory requirements or common law principles support the disclosure or withholding of information;

H) Information is only shared when and where it is necessary and justified for a lawful and specified purpose;

I) Only the minimum identifiable information that is required for the purpose is shared. The information shared should be relevant, proportionate and not excessive for specified purpose, and be defined by the appropriate Tier 2 Protocol.

J) Wherever possible statistical or aggregated and anonymous information is provided, to eliminate the risk of individuals being identified;

K) Only information actually needed for the purpose will be collected or shared;

L) Information is clearly identified as being fact, opinion, or a combination of the two;

M) Information is only used for the purposes for which it was collected or shared;

N) Information is kept and shared safely and securely, with appropriate safeguards in place to ensure only individuals with a legitimate right have access to it, preventing accidental or deliberate unauthorised access;

O) Information no longer needed for legal or administration requirements is disposed of in a safe and appropriate manner;

P) The capacity of a data subject, including children and vulnerable adults, to exercise their right to provide or refuse consent will be considered on an individual case by case basis; and

Q) Considerations of confidentiality and privacy will not automatically cease on death.

6 Tier 2 - Strategic Purpose Information Sharing Protocols

6.1 The focus of each Protocol is the particular **purpose** underlying the need to share, potentially across boundaries, specific sets of personal information. The organisations signing up to a Protocol become members of an 'Information Community' for that purpose. While a signatory organisation can be a member of several communities, it will not always be appropriate or necessary for them to sign up to every protocol.

6.2 Each Protocol describes the common contexts and shared objectives between signatory organisations delivering services of a similar scope, defines the type of information to be shared within that community, the purposes for which it can be shared, and the underpinning legislation and the associated duties and powers that enable legally justifiable exchanges of information for that purpose based on the principles and standards set out in the Charter.

6.3 Tier 2 Protocols will be signed on behalf of signatory organisations by Service Directors or equivalent.

7 Tier 3 Operational Management Information Sharing Agreements

7.1 The third tier agreements underpin each protocol and define the **processes** by which information will be exchanged, monitored and managed between individual signatory organisations within the Information Community. They will identify how requests for information may be made, the information to be shared and the methods of auditing who has had access to information and why. The Agreements will clearly identify who is responsible for managing and monitoring the information sharing and the named lead officer for any queries.

7.2 In the event of organisational change, only these detailed agreements will need to be reviewed or amended; where information communities contain several partners who provide the same services but who have different internal structures these detailed agreements allow for local variation while maintaining the integrity of the information required.

7.3 Tier 3 Agreements will be signed on behalf of signatory organisations by a senior manager, with responsibility for operational delivery.

8 Signatory organisations to this Charter

8.1 A list of the organisations that have signed up to this Charter, and have agreed to adopt the principles and standards set out in the overarching Policy and the supporting Protocol and agreements is available on the Humber data observatory website (www.humberdataobservatory.org.uk).

9 Complaints

9.1 A complaint from a data subject or their representative about information held under the terms of this Charter will be investigated first by the signatory organisation receiving the complaint.

9.2 Where a complaint identifies that any part of the Charter needs to be reviewed, this action must be taken by the Humber Information Governance Group.

10 Freedom of Information

10.1 The Freedom of Information Act and Environmental Information Regulations gives a general right of access to the information public authorities hold. Any requests for information in relation to the Charter must be passed to the signatory organisation's Freedom of Information Officer to deal with. In signatory organisations not subject to the Act or Regulations the request must be passed to the Humber Information Governance Group.

10.2 Requests for copies of the Charter and Tier 2 Protocols will be directed to the Humber data observatory website (www.humberdataobservatory.org.uk) where they are proactively published.

10.3 Requests for Tier 3 Agreements will be considered on a case by case basis by the signatory organisation to the Agreement, as they will include sensitive information, which could compromise the procedures in place for the security and protection of the personal information.

11 Monitoring and Review

11.1 As a signatory to the Charter we agree to support the Humber Information Governance Group with the monitoring and annual review of the Charter and associated Tier 2 Protocols and Tier 3 Agreements.

12 Humber Information Governance Group

12.1 The Humber Information Governance Group is a virtual Group representing and reporting to the Local Partnership bodies for the City of Hull, the East Riding of Yorkshire, North East Lincolnshire and North Lincolnshire.

13 Partnership undertaking

13.1 As a signatory to the Charter we accept the principles laid down in this document will provide a secure local framework between the signatory organisations for the secure sharing of personal information in a manner compliant with statutory and professional responsibilities.

13.2 On behalf of the organisation I represent, I confirm that we will undertake to comply with all relevant legislation and requirements relating to confidentiality, safe information sharing and disclosure, appropriate storage and destruction of information.

a) Implement and adhere to the standards and principles set out in this Charter whenever exchanging personal information, both with a co-signatories and other organisations;
b) Ensure that all Protocols and Procedures established for the sharing and confidentiality of information are consistent with this Charter;
c) Co-operate, as far is compatible with existing statutory responsibilities, with other signatories to ensure effective information sharing and reduce duplication.

13.3 Signatories

Signature: [signature] Name: SIMON DRIVER

Position: CHIEF EXECUTIVE, NORTH LINCOLNSHIRE COUNCIL

Signature: Name:

Position:

Organisation:

Date:

Appendix A Tier 2 - Strategic Purpose Information Sharing Protocol template

1. Introduction

Introduces the Protocol, and provides details of what the information will be used for and who it will be used by

2. Objectives

Identifies what the Protocol is aiming to achieve through the sharing of personal information.

3. Roles and Responsibilities

Identifies for the sharing of information under the Protocol of

- Who will disclose it;
- What will be disclosed;
- How it will be disclosed and when;
- Who will receive it;
- Who will have access to;
- What it can be used for;
- How it should be stored; and
- When it should be disposed of.

This will be further expanded in the Tier 3 agreements supporting the Protocol.

4. Legislation

The relevant legislation and powers that enables the sharing of information for the purpose specified under the Protocol.

5. Client Consent

The procedures for sharing information, when consent is required and nature of the consent required

6. Monitoring / Review

The specific arrangements in place to review the Protocol and handle complaints.

7. Signatories

The signatories to the Protocol.

Appendix B Tier 3 - Operational Management Information Sharing Agreement template

1. Introduction

Introduces the Agreement, linking to the Tier 1 Charter and Tier 2 Protocol.

2. Legislation

The specific legislation allowing the sharing of information, referencing the Tier 2 Protocol

3. Data Controllers

- Who the Data Controllers are
- How Subject Access Request will be handled

4. Information Format and Quality

- The format and detail of the information to be shared
- Procedures for Quality Assurance

5. Information Security and Confidentiality

- The procedure for making requests and the arrangements for access to information and restrictions including those for third party access
- The storage standards
- The retention and destruction arrangements
- The procedures in place for the secure transfer of data

6. Client Consent to Share Information

- Details of the consents required including obtaining consent, withdrawal of consent, disclosure without consent
- Privacy / Fair Processing Notice requirements

7. Roles and Responsibilities

The lead officers for each signatory organisation and the specific roles and responsibilities within the organisation, including sub organisations

8. Monitoring / Review

The specific arrangements in place to review the agreement and handle complaints.

9. Signatories

The signatories to the agreement.

This page has been intentionally left blank

1 COUNCIL Putting our CUSTOMERS 1ST

Information

Security Policy

NORTH LINCOLNSHIRE COUNCIL

www.northlincs.gov.uk

January 2013

CONTENTS

1. Introduction

Information stored and processed by the council or by third parties working on behalf of the council is a valuable asset. Without adequate levels of protection, confidentiality, integrity and availability of information, the council will not be able to fulfil its obligations including the provision of government services and meeting legal and statutory requirements.

The council's information is in many forms including:

- Hardcopy documents on paper and sent by fax
- Electronic information stored on computers, remote servers, mobile devices, tapes, microfilm, CDs, external disks and USB portable storage devices
- Verbal information (face to face conversations and over the telephone)

We are committed to preserving the confidentiality, integrity and availability of our information assets:

- For sound decision making
- To deliver quality services to our customers
- To comply with the law
- To meet the expectations of our customers and citizens
- To protect our reputation as a professional and trustworthy organisation
- To safeguard against fraudulent activity

This policy is part of a suite of information management policies. It sets out the council's commitment to information security and provides the guidelines and frameworks for ensuring all forms of information, supporting systems and networks are protected from security threats such as malicious software, unauthorised access, computer misuse, information technology failures, human error and physical security threats.

2. Purpose

The purpose of this policy is to protect the council's information assets from all threats whether internal or external, deliberate or accidental. The policy sets out the controls and requirements that will protect a wide range of information that is generated, shared, maintained and ultimately destroyed or archived.

The purpose of security in an information system is to preserve an appropriate level of:

- **Confidentiality:** to prevent unauthorised disclosure of information
- **Integrity:** to prevent the unauthorised amendment or deletion of information
- **Availability:** to prevent unauthorised withholding of information or resources

3. Scope

This policy applies to all information assets held by the council irrespective of their format and covers all locations into which North Lincolnshire Council information is taken and/or accessed.

The scope of this policy extends to:

- Staff and elected members
- Contractors, agencies and partner organisations operating on behalf of the council or on council premises

The policy does not apply to those schools with delegated powers, unless adopted by the governing body.

4. Legal Framework

The council must comply with all relevant statutory UK and European Union legislation, including:

- Human Rights Act 1998
- Data Protection Act 1998
- Freedom Information Act 2000
- Common law duty of confidence
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Environmental Information Regulations 2004

- Regulation of Investigatory Powers Act 2000
- Health & Social Care Act 2001
- Health and Safety at Work Act 1974
- Telecommunications (Lawful Business Practice) Regulations 2000
- Re-use of Public Sector Information Regulations 2005
- Protection of Freedoms Act 2012
- Waste Electrical and Electronic Equipment (WEEE) Directive

The requirement to comply with this legislation extends to everyone, as set out in roles and responsibilities, who are held personally accountable for any breaches of information security for which the council is responsible. This list is not exhaustive and may change over time.

Counter Fraud

In the wrong hands information can easily be used to carry out a fraud within the council, or against others the council carries out business with.

5. Technical Compliance

The head of IT will ensure that information systems are checked regularly for technical compliance with relevant security implementation standards including:

- Government Connect (GCSx/PSN) Code of Connection
- NHS Information Governance Toolkit including N3
- Payment Card Industry Data Security Standard (PCIDSS)
- Information Security Management System Requirements ISO27001
- Code of Practice for Information Security Management ISO17799
- BIP 0008 (Code of Practice for Legal Admissibility in Court)

Operational systems will be subject to technical examination to ensure that hardware and software controls have been correctly implemented.

6. Linkages with other policies and procedures

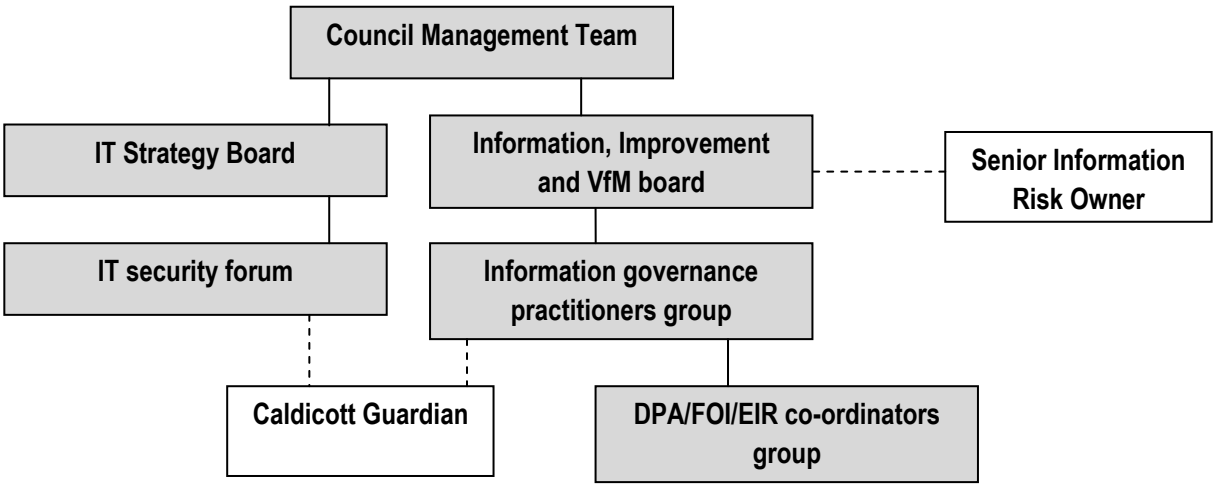
This policy is supported by more detailed policies, standards and procedures. These include but are not limited to the following:

- Human resources policies and procedures:
    - Recruitment
    - Employee induction
    - Disciplinary policy
    - Home working, lone working, remote working
- Information Management Policy
- IT technical security standards
- Employee Code of Conduct
- Digital Technologies Policy
- Data breach Policy
- GCSx Code of Connection
- Humber Information Sharing Charter
- Business Continuity Plan
- Counter Fraud Strategy
- Government Protective Marking Scheme (to be implemented in 2013-14)

Compliance with this policy is essential to reduce fraudulent access to sensitive information. In addition staff must adhere to any specific policies set out for their service areas.

7. Reporting structure

The diagram below illustrates the governance framework and reporting structure for information security:



1. The council's Senior Information Risk Owner (SIRO) is the senior responsible officer for information risks and leads the organisations response. The SIRO is the focus for the management of information risk and reports into the Information, Improvement and VfM board. The SIRO also:

    - Fosters a culture for protecting and using data
    - Provides a focal point for managing information risks and incidents
    - Is concerned with the management of all information assets

2. The Information Governance Officer deputises for the SIRO and is the corporate data protection officer.
3. Caldicott guardian is an advisory role in social services and the NHS and is the conscience of the organisation. Their role is to manage [service users] confidentiality and information sharing issues. The Caldicott Guardian is part of the People directorate and reports into both the IT security forum and the information governance practitioner's forum.
4. The Council Management Team is responsible for ensuring that all employees, with legitimate access to information held by the council are familiar and compliant with their responsibilities under the Data Protection Act 1998.
5. Senior officers are also responsible for ensuring that contractors, partner organisations and third parties have appropriate and satisfactory systems and procedures in place and agreed to terms and conditions consistent with the Information Security Policy before doing business with us.

6. Directorate Co-ordinators [DPA/FOI/EIR] are responsible in their directorates for the co-ordination and processing of information requests in line with legislative requirements.

7. Information asset owners are responsible for undertaking information risk assessments, implementing appropriate controls, recognising actual or potential security incidents and ensuring that policies and procedures are followed. The information asset owners will attend occasional information governance practitioners group.

8. Line managers shall be responsible for ensuring their staff trained to the appropriate level and comply with this policy. All staff have a responsibility for information security.

8. Key Policies and Procedures

Procedure	Summary
Home working / remote working	• Any laptop or other device that is taken off council premises must be encrypted to the user. • All necessary precautions must be taken to ensure the security of hard copy documents that are taken off council premises. • All home working and remote working should be carried out in compliance with the home working policy and have the authorisation of the relevant line manager.
Procurement of services	• Ensure that data protection requirements are clearly specified within the conditions of contract and service specification for all relevant procured services. • Ensure that the council's conditions of contract relating to data protection, freedom of information etc are included in all relevant procurement information. • Ensure that the pre-qualification/evaluation of prospective suppliers includes where appropriate consideration of capability for ensuring data protection. • Ensure that due regard is given to data protection as part of contract monitoring and management. • Consider the implications of sub-contracting and ensure that the above requirements are passed through the relevant supply chain. • Ensure that third parties have adequate controls in place with regards to off site/remote storage of council information.
Disposals	• To comply with the Waste Electrical and Electronic Equipment (WEEE) Directive and ensure that sensitive data is not accidentally released the disposal of any IT and associated equipment must be carried out by IT services. • When disposing of any sensitive and confidential information you

	must use the council's corporate confidential waste facility. • If working at home be aware that you need to comply with the above disposal methods which ensures secure methods such as cross-cut shredding. If no secure disposals methods are available, sensitive information should be transported to a council office for secure disposal. • It is important to keep the waste in a secure place until it can be collected for secure disposal. Never put sensitive and confidential waste in any normal waste bins.
Systems and Software	• All information processing systems which are to be used for storing and processing council information must be formally authorised by IT Services. Information asset owners are responsible for ensuring new systems have the necessary validation checks and audit trail and also ensure user acceptance testing is carried out. User access to systems must be adequately controlled using complex passwords and appropriate access rights. User access rights must be regularly reviewed to ensure they are still appropriate. • Users must use a unique username and password for accessing the council's network and information systems. • Users must be responsible for keeping their passwords confidential at all times, and must not disclose passwords to anyone, including their line managers. Written down passwords shall be discouraged, unless documentation is completely inaccessible to other persons. Weak passwords must not be used. • Users must not attempt to access systems or records within systems which they have not been formally authorised to access. • Users must not bypass, disable or subvert system security controls. • Unauthorised equipment must not be connected to the council's network. The only exception being personal devices connecting to the council's 'guest' wireless system. • Computer systems and software must only be used for purposes for which they are designated. • Only software authorised by IT should be loaded onto the council's computers. Active scanning will automatically check all media plugged into USB ports. • Software must only be used in compliance with the terms of any contractual or licence agreements. • The council will have sole ownership and copyright of all programs and data it has developed. Unless prior written consent is given otherwise. • Deliberate unauthorised access to, copying, alteration or

	interference with computer programs or data is strictly forbidden. • All staff with IT access must undergo the council's Information security e-learning package. Managers will ensure this is part of a new employees' induction. • Managers must ensure that when any staff leave, all council equipment (including their ID card) is returned. IT Services must be informed of all leavers to ensure network access is revoked. • All users must inform their manager if they detect, suspect or witness an incident which may be a breach of security. • All users must be aware that the network is monitored. IT Services will monitor day to day access to ensure adequate protection against security threats, and where necessary, will collect evidence of misuse and unauthorised activity. .
Information Handling	<u>Storage</u> • Everyone must ensure that information is not put at risk of damage or theft, and is stored securely and access allowed only to those who need it for legitimate purposes and in accordance with the Data Protection Act 1998. For example: o Records can be stored in secure buildings with access controls to the building, specific floors and individual offices o The location of any stored records should be sited to avoid unauthorised access, damage, theft and interference. o Stored records must not be removed or moved to another location without notification being given to the relevant information owner o Electronic information needs to be stored on the council network unless alternative storage (e.g. Cloud) is authorised by IT. <u>Communication</u> • Extra care should be taken when printing sensitive information or sending/receiving faxes. When sending sensitive information a test fax should be sent prior to sending the information. In areas without multi-functional devices ensure printed sensitive information is not left unattended. • Voicemail may contain personal and sensitive information and therefore passwords should be kept secure <u>Portable hardware including laptops, mobile devices & tablets</u> • Equipment taken off site must be locked away and kept out of sight when left unattended. • Users shall ensure that unauthorised persons are not able to view council information on portable devices and shall protect access

	by locking computers when unattended. This policy also applies to staff accessing council information on own devices. • Staff must ensure they do not leave portable media such as CDs that contains personal or sensitive information in drives <u>Records Management</u> • Records are a key resource for the effective operation and accountability of the council. It is also recognised that some records will over time become of historical value and need to be identified and preserved accordingly. The information management policy sets out the records management framework for:- o Record creation o Record classification scheme o Record maintenance o Retention and disposal o Access o Management of electronic records • Hardcopy archived records must be stored in the corporate archives. <u>Removable media</u> • To prevent data loss the use of USB devices such as portable hard drives and removable media (such as CDs, DVDs, memory sticks etc) on councils PCs should not be used to store personal and sensitive information unless there is a business requirement to do so. • Staff must only use mobile media to transfer personal and sensitive council information if there is a business requirement to do so and there is no other more secure means available e.g. Government secure GCSx email. • Only media purchased through the councils IT service and with a sufficient level of encryption, may be used to temporarily hold personal and sensitive council information. <u>Office/desk security</u> • Staff should maintain a clear desk policy and ensure that all personal and sensitive information is stored securely and ensure that: o Personal and sensitive information including phone numbers, passwords, financial records, notes on meeting times, places and subjects are not left unattended o Mobile phones can contain sensitive personal information and have their call histories compromised and therefore should be kept secure at all times and not left unattended

	○ Keys and access cards should not be left unattended as they can give intruders access to restricted areas ○ Positioning of desks, furniture and visual display boards should be carefully considered to prevent sensitive information being visible to unauthorised people. ○ Personal and sensitive information should not be left on white boards or notice boards. ○ When leaving desks for short periods all users must us 'Ctrl, Alt and Delete' to lock computers. When leaving desks for long periods users must ensure they are logged off the network.
Protective marking scheme (to be introduced during 2013/14)	The national Government Protective Marking System (GPMS) provides a framework for handling public sector information and to recognise the security required for the information being held, processed or transmitted. Each protective marking is given an appropriate impact level. This is used to determine how much protection these assets should be given. The person handling the information must consider the impact of it being released outside its normal channels, or the impact of its loss or destruction. The GPMS impact levels are: ○ Top Secret ○ Secret ○ Confidential ○ Restricted ○ Protect ○ Not protectively marked The council is currently developing a protective marking scheme which will be introduced during 2013/14.

9. Data Sharing

As set out in the information management policy personal, personal sensitive and confidential information will be shared with the council and with other organisations in line with the law and only where there is a need or obligation to do so. Where there is a need to enable service delivery with external organisations the information sharing will be governed either under the terms of a contract or an information sharing agreement. The council will also share information as required by law.

Contracts with third parties and their own subcontractors must comply with the council's information governance framework.

10. Security Incidents

Any loss of sensitive and confidential information, either actual or suspected, must be reported immediately to the relevant line manager or theirs if they are not available. The incident will be handled in line with the data breach policy. The SIRO will notify other parties, such as the Information Commissioner, as required by legislation.

11. Risk, quality and Audit

The council will ensure that information is accurate at the time of capture and will be subsequently maintained to ensure accuracy, integrity and consistency across systems and datasets as set out in the council's Data Quality policy.

Risk

The SIRO will have overall responsibility for risk management. This will include:

- Maintaining a corporate information management risk register
- Conducting a risk assessment
- Applying risk mitigation in context with business demands
- Measuring results and improving the process from lessons learned
- Implementing training and awareness programmes
- Implementing procedures for the detection and control of security events and incidents

Quality Assurance and Audit

The information security policy, standards and procedures will be audited periodically as part of the annual internal audit work plan.

12. Monitoring and Review

The current version of this policy can be found on intralinc and the council website along with information supporting this policy. This policy and all supporting procedures will be reviewed as it is deemed appropriate but no less frequently than every 12 months.

North Lincolnshire Council
Data Protection Breach Policy

Introduction

1.0 Policy Statement

North Lincolnshire Council is legally required under the Data Protection Act 1998 to ensure the security and confidentiality of data processed on behalf of the public and employees. This legal requirement also covers any data processed by another organisation on behalf of the council. Every care is taken to protect personal data and to avoid a data protection breach. In the unlikely event of data being lost or shared inappropriately, it is vital that appropriate action is taken to minimise any associated risk as soon as possible. The council will follow a Breach Management Plan in the event of a data breach.

2.0 Purpose

The purpose of this policy is to ensure that a standardised management approach is implemented throughout North Lincolnshire Council in the event of a data breach.

3.0 Scope

This policy applies to all personal and sensitive personal data, as defined by the Data Protection Act 1998, processed by the council or on behalf of the council. Schools may choose to adopt this policy but where this is not the case it is expected that they will have their own appropriate policy.

4.0 Implementation and Review Schedule

This policy takes effect immediately. All managers should ensure that staff are aware of this policy and its requirements. If staff have any queries in relation to the policy they should discuss these with their line manager or the Information Management Team.

This policy may need to be reviewed after a breach or after legislative changes, new case law or new guidance. Ordinarily this policy should be reviewed on an annual basis.

5.0 Legislation

The council has an obligation to abide by all relevant UK and European legislation. The acts, which apply, include but are not limited to: -

- Data Protection Act 1998.
- Data Protection EU Directive 95/46/EC
- Criminal Damages Act 1971.

The Data Protection Act 1998 provides a regulatory framework for the processing of information relating to individuals, including the holding, use or disclosure of such information.

Principal seven of this Act requires that an organisation comply with the following for personal data: -

> *Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.*

6.0 Types of Breach

A Data Protection breach could be defined as the unintentional release of personal or sensitive personal data to an unauthorised person, either through accidental disclosure or loss/theft of the information/data. Some examples are: -

- Loss or theft of data or equipment on which data is stored.
- Inappropriate access to data.
- Equipment failure.
- Human error.
- Unforeseen circumstances such as fire or flood.
- Hacking.
- 'Blagging' offences where information is obtained by deception.

Responsibility of Council Departments

7.0 Identification and Classification

This section involves identifying a breach, taking immediate mitigating action and passing this information to the Information Management Team.

7.1 The person who discovers/receives a report of a breach must inform a senior manager. This should ideally be the senior manager responsible for the department in which the breach has occurred, but if this is not possible another senior manager should be informed. If the breach occurs or is discovered outside normal working hours this should be done as soon as practicable. The senior manager must report any data protection breaches to the Information Management Team, again as soon as possible.

7.2 Details of the incident must be accurately recorded and the following information must be provided to the Information Management Team, using the form shown as Appendix A: -

- Date and time of breach / period of time breach occurred.
- Date and time breach detected.
- Who reported the breach.
- Description of the breach.
- Type of breach (See section 6.0).
- Approximate number of data subjects affected.
- Details of any council ICT systems or third party systems involved.
- Details of any action taken to minimise / mitigate the effect on the data subjects
- Details of anyone who is aware of this data breach.
- Brief details of supporting material held by the service – material which either confirms the breach or is related to the breach.
- Details of any contractors or sub contractors involved.

Joint Responsibility between Departments & Information Management

8.0 Links to other Departments

Sometimes a data breach will be identified during an internal investigation under another council policy. Alternatively during a data breach investigation it may be found necessary to inform another council department of the breach.

8.1 Officers indentifying a data breach, as part of another policy investigation, should complete the Data Breach form shown in Appendix A and forward this to a senior member of the Information Management Team. The Information Management Team will provide advice and support in completing the form. When this investigation is complete relevant details should be provided.

8.2 Where a data breach occurs which may affect another department or a school, the Information Management Team will contact the relevant senior manager or school.

Responsibility of Information Management

9.0 Breach Management Plan

The Information Management Team will lead all data breach investigations and will follow the Information Commissioner's Office (ICO) suggested Breach Management Plan: -

1. Containment and recovery.
2. Assessment of ongoing risk.
3. Notification of breach.
4. Evaluation and response.

9.1 Containment and Recovery

Containment and recovery involves limiting the scope and impact of the data protection breach, and stemming the breach as quickly as possible.

9.1.1 A senior member of the Information Management Team will inform the relevant Director(s) and Legal Services.

9.1.2 A senior member of the Information Management Team will ascertain who should contact whom both within the council and externally. If illegal activity is known or is believed to have occured, or where there is a risk that illegal activity might occur in the future a Director in conjunction with a senior member of the Information Management Team and the Head of Audit, Risk and Insurance must consider whether the police need to be informed. An example of illegal activity is theft.

9.1.3 A senior member of the Information Management Team will lead an investigation and to do so will create an Investigation Team, made up of key officers, including Internal Audit. Where contractual arrangements with other organisations are involved advice will be sought from Legal Services about how to proceed and the investigation will be led in conjunction with the Contract Manager.

9.1.4 A senior member of the Information Management Team will work with the Investigation Team to quickly take appropriate steps to ascertain full details of the breach, determine whether the breach is still occuring, recover any losses and limit the damage. Steps **might** include: -

- Attempting to recover any lost equipment or information/data.
- Shutting down an ICT system.
- Contacting the council's Contact Centre and other key departments so that they are prepared for any potentially inappropriate enquiries about the affected data subjects.

If an inappropriate enquiry is received staff should attempt to obtain the enquirer's name/contact details and confirm that they will ring the enquirer back.

- The Information Management Team organising, with the approval of the Communications Team, for a council-wide email to be sent.
- Contacting the Communications Team so they can be prepared to handle any press enquiries or to make any press releases.
- The use of back-ups to restore lost, damaged or stolen data.
- If bank details have been lost/stolen consider contacting banks directly for advice on preventing fraudulent use.
- If the data breach includes any entry codes or passwords then these codes must be changed immediately, and the relevant organisations and members of staff informed.

9.2 Assessment of Ongoing Risk / Investigation

The next stage of the management plan is for the Investigation Team to investigate the breach and assess the risks arising from the breach.

9.2.1 The Team should ascertain whose data was involved in the breach, the potential effect on the data subject and what further steps are required to remedy the situation.

9.2.2 The investigation should consider: -

- The type of data.
- Its sensitivity.
- How many individuals are affected by the breach?
- What protections are in place (e.g. encryption)?
- What happened to the data?
- Whether the data could be put to any illegal or inappropriate use.
- What could the data tell a third party about the individual?
- How many people are affected?
- What types of people have been affected (the public, suppliers, staff etc)?
- Whether there are wider consequences to the breach.

9.2.3 A senior member of the Information Management Team should keep a clear report detailing the nature of the breach, the assessment of risk/investigation, and the actions taken to mitigate the breach, any notifications made and recommendations for future work/actions.

9.2.4 The initial investigation should be completed urgently and wherever possible within 24 hours of the breach being discovered/reported. A further review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved

9.3 Notification

9.3.1 A senior member of the Information Management Team, after seeking legal advice and working with the Investigation Team should decide whether anyone, such as the Information Commissioner's Office (ICO) or the data subjects, should be notified of the breach. A senior member of the Information Management Team will make any notifications to the ICO. The Investigation Team will decide whether and how anybody else should be notified. Directorates must not make any notifications directly.

9.3.2 Every incident will be considered on a case-by-case basis but if the breach is significant and involves personal or sensitive personal data the ICO should be notified. There is guidance on the ICO website about how and when to notify - www.ico.gov.uk and the following points will be used to assist with this decision: -

- Do we have any legal/contractual obligations in relation to notification?
- Would notification help prevent the unauthorised or unlawful use of the personal data?
- Could notification make the unauthorised or unlawful use of the personal data more likely?
- Could notification help the data subject – could they act on the information to mitigate risks?
- If the data is personal or sensitive personal in nature and there are large numbers of data subjects involved or possible serious consequences we should notify the ICO.
- The dangers of over notifying, which may cause disproportionate enquiries and work.

9.3.3 Notifications should include a description of how and when the breach occurred, what data was involved and what has already been done to mitigate the risks.

9.3.4 When notifying data subjects, specific and clear advice should be given on what individuals can do to protect themselves and what the council can do to assist them.

9.3.5 Details should be provided of how to make a complaint to the council.

9.4 Review and Evaluation

Once the initial after effects of the breach are over a senior member of the Information Management Team should fully review both the causes of the breach and the effectiveness of the response to it and work with Internal Audit to determine if any further control improvements are required.

9.4.1 The Head of Information Management will write a report for the Council Management Team (CMT).

9.4.2 If issues are identified an action plan must be drawn up to put these right.

10.0 Information Management Contact Details

Please do not leave a voicemail or an email to report a data breach. Always speak with somebody in the Information Management Team. The main contacts are: -

Principal Business Analyst (Information Management) – Phillipa Thornley
Telephone: 296302
Email: phillipa.thornley@northlincs.gov.uk

Head of Information Management – Chris Daly
Telephone: 296161
Email: chris.daly@northlincs.gov.uk

Appendix A **Data Breach Form**

Contact details of person submitting form

Name	
Job Title	
Address	
Telephone Number	
Email Address	

Incident Information

Date / Time of Breach or Period of Time

Date / Time Breach Detected

Who / What Reported the Breach?

Description of the Breach

Type of breach – see section 6.0 for list: -

Approximate number of Data Subjects affected

Details of Council ICT / 3rd Party ICT Systems Involved

Details of any action taken to minimise / mitigate the effect on the data subjects

Who is aware of this data breach?

Brief Details of Supporting Information held by Department

Details of any Contractors / Sub Contractors Involved



DATA QUALITY

Corporate Policy

North Lincolnshire Council

UPDATED AUGUST 2011

NORTH LINCOLNSHIRE COUNCIL

www.northlincs.gov.uk

DATA QUALITY

Corporate Policy

Contents

Version Control

Date	Reason for change
June 2010	Both protocol and policy updated to reflect new national guidance, links to spot check questions, recommendations from the Audit Commission and Internal Audit and links to new auditing method developed by the performance team.
March 2011	Updated to reflect changes to the National Context and to include references / links to useful documents / web sites.
August 2011	Updated to reflect changes to the corporate performance framework and data quality expectations.

INTRODUCTION TO DATA QUALITY

Introduction

This Policy sets out North Lincolnshire Councils approach to securing improved performance management through good quality data. Data quality is an essential ingredient for reliable performance and financial information. Performance and financial information is crucial to Council Officers, Members and partners as a tool to assess performance and for decision making. This information must be fit for purpose, appropriate, accurate and reliable. This will ensure that the Council and its partners are able to reliably demonstrate how they are currently performing, describe how they will deliver improved service outcomes and inform future decisions regarding funding and service delivery.

This Data Quality Policy will ensure staff at all levels who have a responsibility for collecting, analysing, manipulating or using data and information:

- ✓ Have a greater awareness of data quality and their responsibilities.
- ✓ Recognise the importance for good quality data, and how they contribute to it
- ✓ Have the knowledge and competencies to produce good quality data and information

From May 2010, under the new coalition government, there will no longer be a Use of Resources assessment to test our data quality arrangements. There is expected to be a likely reduction in demand by central government for data and a re-emphasis on local performance, coupled with less inspection and external review of council's systems and procedures. However, the council is committed to data quality and continues to support the standards set out by the Audit Commission. It is vital that the authority does not allow the focus on the quality of local data to decline. The better managed authorities will continue place an emphasis on ensuring the data they need for their own decision making and for external accountability remains of high quality. As there will be less benchmarking to identify errors it is important that our local PI's have the same level of Data Quality.

This policy will provide a ready source of reference to support such practices. However, as circumstances change, it is inevitable that new thinking and approaches will emerge.

In the meantime, this policy, various forums and guidance documents, communities of practice and other sources of reference should be utilised to ensure the drive for high quality data underpins all aspects of our services.

What is Data quality?

Data is an essential part of the performance management arrangements of any service or organisation. It can be broadly defined as being "any type of statistic, fact or piece of information"; however data should never be collected simply because it is available. It should be collected and used to enable services to demonstrate how they are currently performing and describe how they will improve

The terms 'data', 'information' and 'knowledge' are frequently used interchangeably. Data quality focuses on data; that is, the basic facts from which information can be produced by processing or analysis.

Definitions

Terminology	Definitions
Data	Data are numbers, words or images that have yet to be organised or analysed to answer a specific question.
Information	Produced through processing, manipulating and organising data to answer questions, adding to the knowledge of the receiver.
Knowledge	What is known by a person or persons. Involves interpreting information received, adding relevance and context to clarify the insights the information contains.

Data is collected by services for several reasons:

- Measure progress towards achieving targets, outcomes and priorities
- Identify areas where they are performing well and areas where they need to improve
- Set targets and identify future outcomes and priorities for departments and the organisation as a whole
- Compare current performance with performance historically
- Compare performance with the performance of other similar organisations
- Prove accountability to the public, government bodies and to partners
- Inform policy decisions
- Enable correct use of resources
- Understanding customer needs

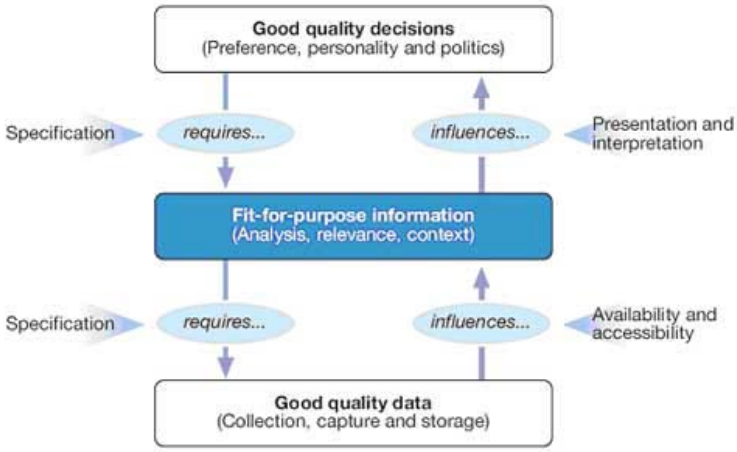
Producing data that are fit for purpose should not be an end in itself, but an integral part of an organisation's operational, performance management, and governance arrangements. Bodies that put data quality at the heart of their performance management systems are most likely to be actively managing data in all aspects of their day-to-day business, in a way that is proportionate to the cost of collection, and turning the data into reliable information for decision making.

In 2008, the Audit Commission published a discussion paper 'In the know, using information to make better decisions'. This identified the quality of data as key to making better decisions, which improves outcomes for local people

The Audit Commission concluded that:

- When decision makers use information well, local public services improve.
- Information needs to be relevant for the decision at hand.
- Good quality data are the foundation of good quality information.
- The way information is presented is important for accurate interpretation.
- Using information well requires decision makers and analysts to have particular skills.
- People need to think carefully about the information they use whenever they make decisions

In order that performance information can be used for these purposes, the quality of the data used must be robust and reliable.



Data quality can be described using six key characteristics or dimensions. These characteristics can help public bodies and their partners to assess the quality of their data and take action to address potential weaknesses

Dimensions of data quality
There are six key characteristics of good quality data.

Accuracy
Data should be sufficiently accurate for their intended purposes, representing clearly and in enough detail the interaction provided at the point of activity. Data should be captured once only, although they may have multiple uses. Accuracy is most likely to be secured if data are captured as close to the point of activity as possible. Reported information that is based on accurate data provides a fair picture of performance and should enable informed decision making. The need for accuracy must be balanced with the importance of the uses for the data, and the costs and effort of collection. For example, it may be appropriate to accept some degree of inaccuracy where timeliness is important. Where compromises are made on accuracy, the resulting limitations of the data should be clear to their users. This must be a judgment determined by local circumstances, and is unlikely to be appropriate in the case of the data supporting published performance indicators.

Validity
Data should be recorded and used in compliance with relevant requirements, including the correct application of any rules or definitions. This will ensure consistency between periods and with similar organisations, measuring what is intended to be measured. Where proxy data are used to compensate for an absence of actual data, bodies must consider how well these data are able to satisfy the intended purpose.

Reliability
Data should reflect stable and consistent data collection processes across collection points and over time, whether using manual or computer based systems, or a combination. Managers and stakeholders should be confident that progress toward performance targets reflects real changes rather than variations in data collection approaches or methods.

Timeliness
Data should be captured as quickly as possible after the event or activity and must be available for the intended use within a reasonable time period. Data must be available quickly and frequently enough to support information needs and to influence service or management decisions.

Relevance
Data captured should be relevant to the purposes for which they are used. This entails periodic review of requirements to reflect changing needs. It may be necessary to capture data at the point of activity which is relevant only for other purposes, rather than for the current intervention. Quality assurance and feedback processes are needed to ensure the quality of such data.

Completeness
Data requirements should be clearly specified based on the information needs of the body and data collection processes matched to these requirements. Monitoring missing, incomplete, or invalid records can provide an indication of data quality and can also point to problems in the recording of certain data items.

Appendix 1 sets out the recommendations from the Audit Commission on the standards that organisations should be working towards to ensure better quality data.

Importance of Data quality

Good quality data is the essential ingredient for reliable performance and financial information. The data must be fit for purpose, representing in an accurate and timely manner an organisation's activity. At the same time, a balance must be achieved between the importance of the information need and the cost of collecting the supporting data with the necessary accuracy, detail and timeliness. To achieve this balance, public bodies need to determine their information priorities and put in place arrangements to secure the quality of the data to satisfy these needs.

The risk in not identifying and addressing weaknesses in data quality, or the arrangements that underpin data collection and reporting activities, is that information may be misleading, decision making may be flawed, resources may be wasted, poor services may not be improved, and policy may be ill-founded. There is also a danger that good performance may not be recognised and rewarded.

The responsibility for ensuring that data are fit for purpose rests with North Lincolnshire Council and its partners. Performance and financial information is crucial to officers, members and partners as a tool for management and decision-making. All public bodies are accountable to Central Government and the community for the public money that they spend. Therefore, the financial and performance information used by services must be appropriate, accurate, reliable, consistent and timely. This will generate confidence that all services are focusing on the key areas for improvement and will ensure that informed decisions are made and service improvement can be achieved. Data quality and therefore the Data Quality Policy are fundamental to the performance management framework of the council and its partners.

Figure 2:

Stakeholders

Key stakeholders and their information needs.

Stakeholder	Information uses
Service users and the public	Exercising choice, understanding the service standards to expect and holding public bodies to account.
Staff in public sector organisations	Delivering services day to day at the front line; the starting point for data collection and use.
Managers in public sector organisations	Monitoring and managing service delivery and benchmarking performance against others.
Local councillors, trust non-executives	Decision making; monitoring strategic objectives, targets and use of resources; ensuring accountability.
Partners	Monitoring the achievement of partnership targets and the use of resources; ensuring accountability.
Commissioners	Identifying population need and determining priorities and services for meeting it; monitoring the achievement of contractual arrangements.
Central government	Developing policy; monitoring progress of new initiatives, and the achievement of national targets; publishing local performance information at national level; identifying poorly performing organisations and rewarding good performance with autonomy and resources.
Regulators	Monitoring performance and use of resources of local bodies; publishing comparative performance information and national studies; planning work programmes proportionate to risk.

DATA QUALITY AT NORTH LINCOLNSHIRE COUNCIL

Our Position

For several years the council has undergone various external assessments of its data quality arrangements.
The assessments looked at how we perform in data quality under various headings:

- Governance and Leadership
- Policies
- Systems and Processes
- People and Skills
- Data use and Reporting

At the end of the assessment a judgement was made based on the following:

4 - Well above minimum requirements - performing strongly
3 - Consistently above minimum requirements - performing well
2 - At only minimum requirements - adequate performance
1 - Below minimum requirements - inadequate performance

Our results:

Data Quality:	2005/06	2	Minimum Requirements - Adequate Performance.
Data Quality:	2006/07	3	Consistently above minimum requirements - performing well
Data Quality:	2007/08	3	Consistently above minimum requirements - performing well.
Use of Resources:	2008/09	2	Performing Adequately (As part of 2.2 UOR Assessment)
UOR VfM:	2009/2010	3	Performing Well (As part of the UOR VfM assessment)

During the 2009/2010 Assessment, The Audit Commission reported they found evidence of service improvement following intervention by performance management and improving data quality for key indicators. The report also stated that we have further improved arrangements, responding to recommendations made in 2008/09 across all KLOE focus points, and our arrangements have demonstrated clear impact. There were no areas identified for improvement.

How do we achieve Data quality?

The Data Quality Policy was developed following recommendations from our external audit. The policy will further enhance the work that is being done at both corporate and service levels. It also supplements the council's performance management framework.

The Council Data Quality Protocol **Appendix 2** was created to improve the quality of data within North Lincolnshire. This has now been reviewed and developed to take into account the new performance framework, recommendations from external audit and guidance from Internal Audit. The protocol has been structured as a checklist, to help services ensure the data and information they produce follows the six key characteristics of good quality data. The protocol has been structured into are 5 key sections General Data quality Management Arrangements, before calculation, during calculation after calculation and target setting.

Process maps should be created for all performance indicators. A process map is a diagrammatical way to define the sequences of activities (processes) that must take place

when calculating a performance indicator result from data collection through to final calculation.

A guidance document is available **(Appendix 3)** to aid in the construction of process maps. It is highly recommended that maps are created based on the guidelines outlined in this document, to ensure a quality, consistent approach across the organisation.

Data verification is required for all priority Indicators. The Performance Management System data quality tool may be utilised for this purpose. Data verification is a vital part of the process and confirms that the indicator has been calculated in compliance with the Data Quality Policy and Protocol, that data has been independently checked and that the data /information are reviewed by senior management.

Partners

The council is committed to working with partners to contribute to achieving each organisations priorities and to deliver joined up public services in order to improve outcomes for the people of North Lincolnshire.

Information used/shared by partners should comply with the Data Protection Act 1998. Any information held may also be subject to requests for disclosure under the Freedom of Information Act 2000.

Services

Services should follow this policy when dealing with data. Not only is it important for ensuring that priority Indicators they are responsible for are correct but all data they use to inform decision making should be sound. If they work with partners and or contractors they should be satisfied that the information that comes from these sources is correct. It would be sensible to put in place a process of reviewing internal and external data, this should be done by setting their own performance indicators for Data quality and conducting audits. Where data comes from an external body that is contracted through the council then the requirements to produce accurate and timely data should be specifically built into the contract terms and conditions.

Awareness & Training

Awareness of Data quality will be raised at the Strategic Performance Group and in one to one meetings with services.

Data quality workshop sessions are available if required for staff involved in data collection and calculation and staff at manager level. The focus of the training is to:

- ✓ Develop greater awareness and understanding of what is meant by data quality.
- ✓ Raise awareness of the content of the Data Quality Policy and Protocol and the importance of data quality across the organisation.
- ✓ Raise awareness of the importance of continual verification (auditing) of indicators to check data quality arrangements
- ✓ Highlight roles and responsibilities for staff in terms of assuring the quality of data and information they use, analyse, supply or have responsibility for.

Data quality is included in both the Corporate and Management Induction Session.
Data quality has now been included in employee generic competencies. Training needs should also be addressed through one to one's and the Employee Appraisal process.

Data quality information, guidance and documentation, including links to other useful websites are on the “Performance” page of the intralinc under “Councilwide issues”, to facilitate sharing and raising awareness.

Performance Management System (PMS)

The Performance Management System is used for holding all performance information and related documents. It is also the basis for performance reports and Service Performance Reviews. The system contributes to performance management of action plans and Indicators which contribute to the delivery of the Councils’ Priorities. This system is available to all officers on the email system and also relevant partners.

All priority indicators are monitored within the Performance Management System. It is expected that each priority indicator as a minimum the following documents attached:

- ✓ Where applicable - definitions for indicators and links to relevant further guidance
- ✓ Process maps and calculations for indicators.
- ✓ All relevant working papers, evidencing the calculations and if applicable source data where the service is involved in calculation of the indicator
- ✓ Target setting forms

The document manager contains national best practice and policy documents.
The Newsroom is used to promote new initiatives and guidance.

Where do we want to be?

Quality data is important; information provides the basis for the majority of work we undertake and informs the planning process. If we do not continue to improve our arrangements then we are at risk of poor decision making and wasting resources.

The council’s aim is to keep reviewing and improving, and to have data quality arrangements which are robust enough to withstand internal and external scrutiny.

ROLES AND RESPONSIBILITIES

All Staff

- Recognise and understand the importance of high quality data, and how they contribute to this.
- Awareness and adherence to the Data Quality Policy and Protocol
- To make recommendations for improvement whenever identified

Improvement & Value for Money Team

- Raise awareness of the principles and importance of good data quality across the council.
- Provide support and guidance to services including provision of regular training sessions.
- Communicate the Data Quality Policy and Protocol
- Ensure that the Data Quality Policy, Data Quality Protocol are updated and maintained.
- Promote the importance of data quality in performance management and decision making when opportunities arise.
- Pro-actively disseminate updated guidance and best practice.
- Reporting of internal and external audits.
- Manage the Performance Management System.
- Facilitate the Strategic Performance Group.
- Review the Performance Framework as required.

Service Data quality Champions

- Raise awareness of the principles and importance of good data quality across the service.
- Ensure a regular programme of audits / reviews are carried out on priority indicators within their service to ensure data quality requirements are being met.
- Communicate the Data Quality Policy and protocol and ensure it is adhered to within the service
- Act as first point of contact for queries regarding data quality for their service.
- Have a thorough understanding of the definition of the indicators they are responsible for, and ensure all relevant staff who have an input into the calculation have an understanding of the definition sufficient to fulfil their roles.
- Act as liaison on data quality matters between the Improvement & Value for Money Team and their service
    - Attend all relevant data quality meetings and workshops, and
    - Ensure key messages are disseminated across the service.
- Ensure every result submitted onto PMS has been subject to data validation and quality assurance checks.
- There is a named deputy officer who can uphold the roles and responsibilities of the data quality champion in their absence.
- Promote the importance of data quality in performance management and decision making when opportunities arise.
- Carry out regular audits on indicators to ensure data quality requirements are being met.

Indicator Editors

- Have an understanding of the relevant indicator definitions and guidance documents sufficient to fulfil their roles.
- Ensure results, target data and relevant information is entered onto the Performance Managements system in line with the timescales specified by the Improvement & Value for Money Team.
- Ensure working papers are attached to every result.
- Ensure there is a clear, evidence based audit trail for the calculation of each performance indicator.

Indicator Owners

- Ensure results, target data and information is entered onto the Performance Managements system in line with the timescales specified by the Improvement & Value for Money Team.
- Ensure concise meaningful supporting commentary is included against indicator results within the Performance Management System, focussing on reasons for current performance.
- Ensure a regular programme of audits / reviews are carried out on priority indicators within their service to ensure data quality requirements are being met.
- Ensure data collection systems and processes are robust, produce reliable data and are fully documented.
- Have a thorough understanding of the definition of the indicators they are responsible for, and ensure all relevant staff who have an input into the calculation have an understanding of the definition sufficient to fulfil their roles
- Ensure every result submitted onto PMS has been subject to data validation and quality assurance checks, in line with the Data Quality Protocol
- Ensure process maps are attached to every indicator with focus on controls in place to mitigate the risk of poor quality data.
- Ensure the Data Quality Policy and protocol is adhered to.
- Monitor and address training needs of staff as they arise.
- Ensure accountability is clearly defined

Indicator Approvers

- Have a thorough understanding of the definition of the indicators they are responsible for approving.
- Ensure every result submitted onto PMS has been subject to data validation and quality assurance checks, in line with the Data Quality Protocol
- Mark results in the Performance Management system as approved once all relevant checks have been carried out.

Information Providers – Internal (Council)

- Ensure data / information is supplied to the relevant service in line with agreed timescales
- Ensure sound governance arrangements are in place based on risk. For examples, a written agreement / data sharing protocol / Service level agreement / Memorandum of Understanding covering data quality with relevant data providers. A Data Sharing Agreement Template is available on the intralinc. It is recommended services utilise this documentation in all instances of internal data sharing.

- Ensure quality of data produced is of the required standard by following the Council Data Quality Protocol where applicable.

Information Providers – External (Partners)

- Ensure data / information is supplied to the relevant service in line with agreed timescales
- Ensure sound governance arrangements are in place based on risk. For examples, a written agreement / data sharing protocol / Service level agreement / Memorandum of Understanding covering data quality with relevant partners
- Ensure quality of data produced is of the required standard by following agreed standards.

AUDITING AND REPORTING

Auditing

A key element of ensuring sound data quality arrangements is the ongoing audits of priority Indicators. In the past, the Improvement & Value for Money Team have carried out a programme of audits on national Indicators based on a risk spreadsheet of priority measures. These audits were carried out by means of a checklist to ensure that data quality requirements are being met. The checklist was based on guidance from Internal Audit, recommendations from the Audit Commission and researching best practice.
The audit process ensures a robust, evidence based evaluation of the Data Quality controls services have in place.
Following an Audit, the Improvement & Value for Money Team reported all recommendations to relevant staff within the service. These recommendations are followed up to ensure services have put corrective action in place.

As from April 2011 it is expected that ALL services utilise the audit documentation available on the intralinc to carry out a programme of audits on their own priority indicators.

Reporting

Findings of audits are reported to the indicator owners and managers and those that are considered a risk are reported to CMT. Performance working groups have data quality as a standing item on the agenda. The Corporate Quarterly Performance Review also has regular updates.

Further Information

Publications:

- *Improving Information to Support Decision Making: Standards for Better Quality Data*, (Audit Commission, 2007) – Appendix 1
- *In the know: Using information to make better decisions (*Audit Commission, Discussion Paper, February 2008)
- *Is there something I should know? Making the most of your information to improve services* (Audit Commission, Local Government National Report + Self assessment framework, July 2009)
- *Nothing but the truth?* (Audit Commission, Discussion Paper, November 2009)
- *A Managers Guide to Performance Management* (Audit Commission and Improvement and Development Agency for Local Government, 2006).

Web Links:

- Data Quality Community of Practice
  http://www.communities.idea.gov.uk/c/79131/home.do

Appendix 1

The standards for better quality data

(Source "Improving information to support decision making: standards for better quality data" Appendix 1)

These standards are intended for use by public bodies to support improvement in data quality. The standards define a framework of management arrangements that bodies can put in place, on a voluntary basis, to secure the quality of the data they use to manage and report on their activities. The standards distil the principles and practices identified in existing guidance, advice and good practice.

The standards are intended to be used flexibly and proportionately to promote better data quality, recognising local risks and circumstances, rather than as a rigid set of requirements or as a checklist. This means the standards intentionally provide high-level descriptions, recognising that the detail of their implementation is a matter for local judgement. Alternative approaches to achieving these aims may also be appropriate, where they achieve the outcome of securing reliable data to support informed decision making.

1. Governance and leadership

The body has put in place a corporate framework for management and accountability of data quality, with a commitment to secure a culture of data quality throughout the organisation.

Key components:

1.1 There is clear corporate leadership of data quality by those charged with governance.

1.2 A senior individual at top management level (for example a member of the senior management team) has overall strategic responsibility for data quality, and this responsibility is not delegated.

1.3 The corporate objectives for data quality are clearly defined (although this may not necessitate a discrete document for data quality), and have been agreed at top management level.

1.4 The data quality objectives are linked to business objectives, cover all the body's activities, and have an associated delivery plan.

1.5 The commitment to data quality is communicated clearly, reinforcing the message that all staff have a responsibility for data quality.

1.6 Accountability for data quality is clearly defined and is considered where relevant as part of the performance appraisal system.

1.7 There is a framework in place to monitor and review data quality, with robust scrutiny by those charged with governance. The programme is proportionate to risk.

1.8 Data quality is embedded in risk management arrangements, with regular assessment of the risks associated with unreliable or inaccurate data.

1.9 Where applicable, the body has taken action to address the results of previous internal and external reviews of data quality.

1.10 Where there is joint working, there is an agreement covering data quality with partners (for example, in the form of a data sharing protocol, statement, or service level agreement).

2. Policies

The body has put in place appropriate polices or procedures to secure the quality of the data it records and uses for reporting.

Key components:

2.1 There is comprehensive guidance for staff on data quality, translating the corporate commitment into practice. This may take the form of a policy, set of policies, or operational procedures, covering data collection, recording, analysis and reporting. The guidance has been implemented in all business areas.

2.2 Polices and procedures meet the requirements of any relevant national standards, rules, definitions or guidance, for example the Data Protection Act, as well as defining local practices and monitoring arrangements.

2.3 Policies and procedures are reviewed periodically and updated when needed. The body is proactive in informing staff of any policy or procedure updates on a timely basis.

2.4 All relevant staff have access to policies, guidance and support on data quality, and on the collection, recording, analysis, and reporting of data. Where possible this is supported by information systems.

2.5 Policies, procedures and guidelines are applied consistently. Mechanisms are in place to check compliance in practice, and the results are reported to top management. Corrective action is taken where necessary.

3. Systems and processes

The body has put in place systems and processes which secure the quality of data as part of the normal business activity of the body.

Key components:

3.1 There are systems and processes in place for the collection, recording, analysis and reporting of data which are focused on securing data which are accurate, valid, reliable, timely, relevant and complete.

3.2 Systems and processes work according to the principle of right first time, rather than employing extensive data correction, cleansing or manipulation processes to produce the information required.

3.3 Arrangements for collecting, recording, compiling and reporting data are integrated into the business planning and management processes of the body, supporting the day-to-day work of staff.

3.4 Information systems have built-in controls to minimise the scope for human error or manipulation and prevent erroneous data entry, missing data, or unauthorised data changes. Controls are reviewed at least annually to ensure they are working effectively.

3.5 Corporate security and recovery arrangements are in place. The body regularly tests its business critical systems to ensure that processes are secure, and results are reported to top management.

4. People and skills

The body has put in place arrangements to ensure that staff have the knowledge, competencies and capacity for their roles in relation to data quality.

Key components:

4.1 Roles and responsibilities in relation to data quality are clearly defined and documented, and incorporated where appropriate into job descriptions.

4.2 Data quality standards are set, and staff are assessed against these.

4.3 The body has put in place and trained the necessary staff, ensuring they have the capacity and skills for the effective collection, recording, analysis and reporting of data.

4.4 There is a programme of training for data quality, tailored to needs. This includes regular updates for staff to ensure that changes in data quality procedures are disseminated and acted on.

4.5 There are corporate arrangements in place to ensure that training provision is periodically evaluated and adapted to respond to changing needs.

5. Data use and reporting

The body has put in place arrangements that are focused on ensuring that data supporting reported information are actively used in the decision making process, and are subject to a system of internal control and validation.

Key components:

5.1 Internal and external reporting requirements have been critically assessed. Data provision is reviewed regularly to ensure it is aligned to these needs.

5.2 Data used for reporting to those charged with governance are also used for day-to-day management of the body's business. As a minimum, reported data, and the way they are used, are fed back to those who create them to reinforce understanding of their wider role and importance.

5.3 Data are used appropriately to support the levels of reporting and decision making needed (for example, forecasting achievement, monitoring service delivery and outcomes, and identifying corrective actions). There is evidence that management action is taken to address service delivery issues identified by reporting.

5.4 Data which are used for external reporting are subject to rigorous verification, and to senior management approval.

5.5 All data returns are prepared and submitted on a timely basis, and are supported by a clear and complete audit trail.

Appendix 2

DATA QUALITY PROTOCOL

Performance management is a key aspect of the day-to-day operation of a service. Performance information, often in the form of indicators, is a key illustration of how well a service/function is performing in a particular area. This information can be used for a number of purposes such as – monitoring how well a service is performing, to set future targets to drive continuous improvement in how we deliver our services, as a benchmark of performance or cost against other bodies and to inform the residents of North Lincolnshire of how well the council is delivering services. In order that performance information can be used for these purposes, the quality of the data used must be robust and reliable.

In most instances, the exact specification of how a performance indicator must be calculated will be supplied by an external body. If this is the case then the guidelines provided by the external body must be followed precisely and a clear audit trail of how the indicator has been calculated, backed up by hard-copy evidence where appropriate, must be available. In other cases, a service may decide to monitor and review performance information that they feel is more relevant to the council ambitions and local priorities.

Whether performance information is being used by an external body to analyse our delivery of services, or whether it is being used internally to help drive improvement the need for robust, reliable data is clear. With this in mind, this Data Quality Protocol has been produced. The protocol elements take into considerations:

- Key Lines of Enquiry from the Audit Commission, key principles from the Audit Commission joint paper: *Improving Information to Support Decision Making: Standards for Better Data Quality.*
- Audit Commission spot check questions.
- Improvements identified during external audits of our Data Quality arrangements
- Advise and input from Internal Audit function
- Best practice research.

Where practicable, all information and documents should be attached to the Performance Management System.

The protocol has been structured as a checklist, to help you make sure the data you are producing is accurate. This checklist should be used whether the data is being used internally or externally. We have structured the checklist into five sections – General Data Quality Management Arrangements; before calculation; during calculation; after calculation; and target setting.

Documentation is available on the Intralinc which services can use to carry out audits of their priority indicators. The audit documentation mirrors the elements of this protocol therefore by carrying out audits using the template document you are essentially checking your compliance to the Data Quality Protocol. It is expected that ALL SERVICES adhere to the Data Quality Protocol and that all services utilise the available audit documentation to test the robustness of their data quality arrangements.

Ref	Expected Control	Check
1.	**General Data Quality Management Arrangements**	
1.1	To ensure that all indicators have the same standard of data quality it is expected that each indicator will have a file with the same basic information. This will enable any member of staff to pick up the file and be able to complete the return. It will also enable internal or external audit to be carried out more quickly and efficiently. The file should include:	
	• Definition and other relevant guidance documents	
	• Data source – (This is where the data comes from, whether it is manual records; spreadsheets; word documents; information from IT systems etc.) Where the information is held on a computer, the method of extracting the information or the drive it is held on should be recorded.	
	• Process Map (this is a full mapping of the indicator, detailing how data is sourced / collected, what calculations will take place, how information will be recorded, who will carry out the work, who will approve the result, controls in place to prevent human error, erroneous data entry and unauthorised entry or manipulation)	
	• Target Data (An explanation of how the targets have been arrived at and which types of thresholds need to be met.	
	• Copies of external data (copies of data provided by external organisations to back-up the result)	
	• Working Papers (Evidence of how the result was calculated. Evidence to be attached to PMS)	
	Where practicable, as well as having hard copies of the above, information and documents should be attached to the Performance Management System.	
1.2	Ensure the file is accessible to all relevant/responsible staff.	
1.3	Ensure files and systems have adequate controls in place to minimise human error, prevent erroneous data entry and unauthorised entry or manipulation? (For example, password controls, audit trails, number of people able to input data)	
1.4	Evidence of who is accountable for data quality of this indicator	
1.5	Evidence of action taken to address the results of any previous internal or external reviews/audits of data quality.	
1.6	Ensure at least two staff have knowledge of how to calculate this indicator. This ensures cover for absence. The use of process maps to explain how indicator data is produced is recommended as good practice.	
1.7	Ensure the relevant staff (1.6) have received data quality training during the year, or training directly related to data needed for this indicator or service?	

Ref	Expected Control	Check
2.	**Data Quality Protocol Element – BEFORE COLLECTION / CALCULATION**	
2.1	DEFINITION:	
	• Check the various components of the indicator definition are fully understood by the responsible officer. (E.g. what is a "visit" to a library?)	
	• Ensure regular checks carried out to ensure definitions and guidelines are up to date Definitions for National Indicators are attached to the general tab of the indicator in PMS. Services are responsible for checking the definitions of all other indicators that they report.	

Ref	Expected Control	Check
2.	**Data Quality Protocol Element – BEFORE COLLECTION / CALCULATION**	
2.2	Where applicable, have specific guidelines been followed when collecting the data, especially in areas such as: • Method of gathering data • Sampling • Figures carried forward from previous years/time periods • Time period for which data is collected • Geographic locations	
2.3	Ensure use of correct population/household data used to calculate this indicator. For example, use the correct population figure/number of households for the specified time period. The corporate performance team will publish this data on PMS document manager. Details of population/household data source should be kept in the indicator file.	
2.6	Where there is joint working/data sharing (internal or external), ensure there are sound governance arrangements in place based on risk. For example - a written agreement/data sharing protocol/Service level agreement covering data quality with relevant partners / data providers.	

Ref	Expected Control	Check
3.	**Data Quality Protocol Element – DURING CALCULATION**	
3.1	Check the indicator been calculated correctly in accordance with the relevant definitions. If you are using spreadsheets, check the calculation formulae to make sure they are accurate.	
3.2	Check manual intervention is minimised in producing indicator data/results	

Ref	Expected Control	Check
4.	**Data Quality Protocol Element – AFTER CALCULATION**	
4.1	The indicator/data must be supported by a clear and complete audit trail detailing how indicator has been calculated Any reports, documents or statistics used must be clearly cross-referenced and retained. Working papers / audit trail and supporting papers and data evidence must be retained in the indicator file and on PMS	
4.2	Ensure that at the end of each relevant period working papers clearly detailing the calculation of the result are retained and attached to the PMS.	
4.3	Follow the specified dates and methods for submission of the data if applicable (SDL)	
4.4	If revisions are made to data after it has been submitted to the relevant government body, ensure adequate revision controls are in place.	
4.5	Ensure data is reported on PMS promptly in line with the collection frequency required by Improvement and Value for Money Team (CMT reporting)?	
4.6	Results must be subjected to the appropriate levels of verification and senior management approval.	

Ref	Expected Control	Check
5.	**Data Quality Protocol Element – TARGET SETTING**	
5.1	The correct targets should be calculated and recorded on PMS.	
5.2	Do targets meet the SMART criteria? • Specific • Measurable • Achievable • Relevant • Timely	
5.3	Target must in most cases reflect an improvement on the current performance level. Where a target is set that is the same or poorer than current performance, a full explanation of the reasons for this should be included in the indicator file.	

- ✓ If you have concern about the calculation of any of your indicators, contact the Improvement and Value for Money Team. We can then arrange for them to be checked and verified internally, rather than having them reserved by external auditors at a later date.
- ✓ The data and working papers should be available for inspection by internal or external auditors at any time in the indicator file.

If you require any further help or guidance please call Jo Busby on 6512

Appendix 3 PROCESS MAP GUIDANCE

Introduction

A process map is a diagrammatically way to define the sequence of activities that are undertaken within a process. In the context of performance indicators, this will be from the point of data collection, through to data entry into PMS (supported by comparison of the result to the HUB database.) Each individual activity which takes place from the initial point of collection through to calculation and entry onto PMS should be defined, and mapped. Each step is interlinked with arrows which clearly identify the direction or 'flow' of the process.

These guidelines have been developed as a tool to aid the creation of process maps within a service and to ensure a consistent approach is adopted across the organisation when mapping the process for the calculation of performance indicators.

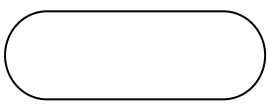
Process Mapping is a key tool utilised for process analysis and redesign for business transformation and improvement. For the purposes of this document the information will be kept simple and will focus primarily on mapping the process for calculation of performance Indicators. Process improvement will be touched on in the final section.

Why process map performance indicators

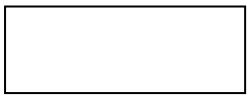
- Constructing process maps promotes better understanding of processes, and better understanding of processes is a pre-requisite for improvement.
- A process maps allows the services to produce a simplified and consistent view of the key activities involved in calculating or extracting indicator results without having to trawl through lengthy guidance documents that may or may not exist.
- Any officer with a level of knowledge within the service will be able to calculate the indicator result and be aware of the expectations in terms of data quality, based on the content of the map.
- Audit Commission data quality guidance states that *"Information systems have built-in controls to minimise the scope for human error or manipulation and prevent erroneous data entry, missing data, or unauthorised data changes".* A process map is an ideal tool for services to clearly identify where there are weaknesses or risks in the process and the controls which have been put in place to mitigate these weaknesses and risks. This will significantly contribute to ensuring data quality arrangements within the service can withstand internal or external scrutiny.
- Can be utilised as a useful training aid new starters and as guidance document, to cover annual leave or other circumstances which may require other staff members to perform the calculations.
- Roles and responsibilities of each activity within a process are clearly defined.
- An important tool in analysing a process and identifying potential areas of waste, and areas where the process could be improved.

Basic Process Map Symbols

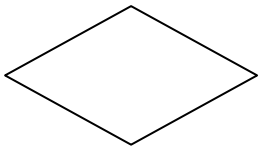
The following three symbols are the most commonly used across all process map design



Terminators show the start and stop points in a process. When used as a start symbol, terminators depict a trigger action that sets the process flow into motion.
When used as an end symbol, terminators depict the point at which the process ends – the 'output'



A **Process** symbol. A rectangle, representing an activity or task. This is the most common symbol in both process flowcharts and business process maps.



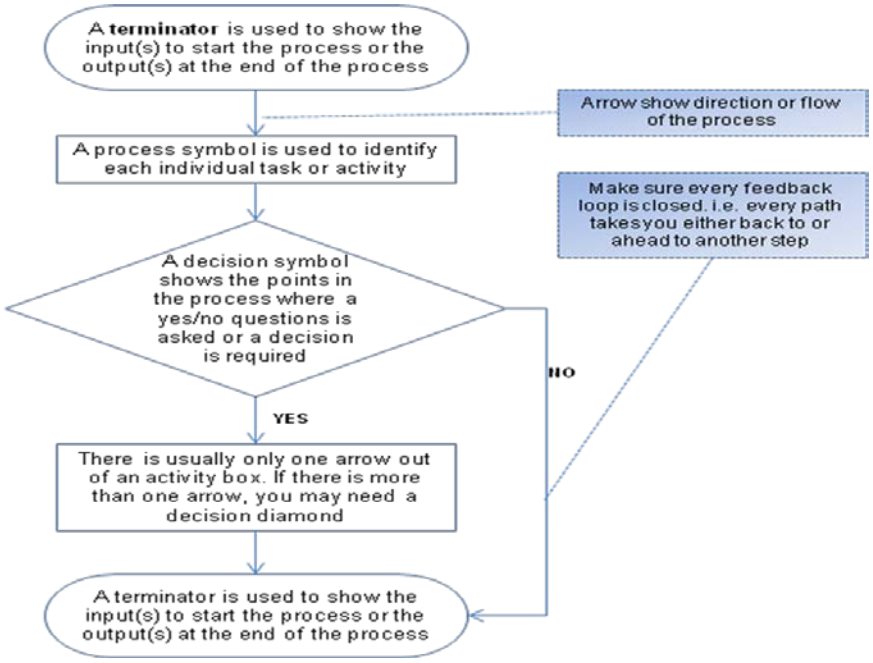
A diamond, representing a **decision**. Typically, a Decision symbol is used when there are 2 options (Yes/No)

Flow line connectors show the direction that the process flows

You may also find it useful, to utilise the following symbol when creating process maps to define document outputs:

A process map step which produces a **document**

The following represents diagrammatically, how the symbols and flow line connectors work together to produce a process map;



Constructing a Process Map

There are no hard and fast rules for constructing process maps, but there are guidelines which are useful to bear in mind to ensure consistency and quality.

Here are six steps which can be used as a guide for completing flowcharts.

1. Start with a 'trigger' event.
2. Note each successive action concisely and clearly. Mapping each of the activities in sequence as they are performed using the appropriate symbols and connecting arrows between boxes to represent the direction.

3. Concisely describe each task or decision in its own box. You may sometimes wish to number (some of) the boxes and provide a key to where the activity is described in more detail.
4. Make cross references to supporting information
5. Follow the process through to a useful conclusion/output.

The map should clearly identify:

WHO does WHAT.

- Limit this to job titles, team names or organisations as appropriate
- Who collects or provides the data?
- Who is responsible for ensuring the data received from third parties (either internal or external) can be relied upon to be accurate?
- Who is responsible for calculating the final result
- Who is responsible for verifying the final result
- Who is responsible for approving the final result

WHAT is done and WHEN,

- How / where is the data required for the calculation sourced/collected?
- Are there robust systems set up for carrying out the final calculations as per the DCLG definition and how is this achieved?
- If no calculations take place internally, where is the final result sourced and how can we be sure of its accuracy?
- What deadlines are in place for data collection, submission to relevant government department and data entry onto the performance management system?

What DECISIONS have to be taken

- At what stage of the process are there two potential branches (usually a YES or NO) for example, a simple question may be is the raw data complete? If YES the process can move on. If NO then there is a loop back into the process to obtain complete information.
- What possible paths follow from each decision?
- Consider that any loop back into the process could be potential inefficiency or waste.

Where are the RISKS and CONTROLS.

- Identify the risks - where is there scope for human error, unauthorised data manipulation, erroneous data entry, missing data, or unauthorised data changes.
- Identify what controls have been or could be put in place to mitigate the risk, for example, the risk of human error can easily be mitigated by ensuring that manual intervention in the calculation of the result is minimised and that calculations are independently checked.
- Ensure risks and controls are clearly identified on the process map

Note:

- ✓ Be sure you map the **AS IS** process, not what you **THINK** it looks like or how you would **LIKE** it to look.
- ✓ Completed Process maps MUST be attached to the general tab of the indicator in PMS

Please refer to **Appendix A** and **Appendix B** for examples of process maps.

Improvement

Having selected and recorded key processes, there is the potential to take this a step further and use the map as a tool to identify process improvement.
At each stage of the process ask yourself, "*why are we doing this?"* And "*Is it essential to the process?"* If you cannot justify why that stage of the process occurs and/or that stage is not essential to the process then you have identifies WASTE. At this point the process can be re-designed to reduce or eliminate waste to become more efficient and effective.

An efficient and effective process will have:

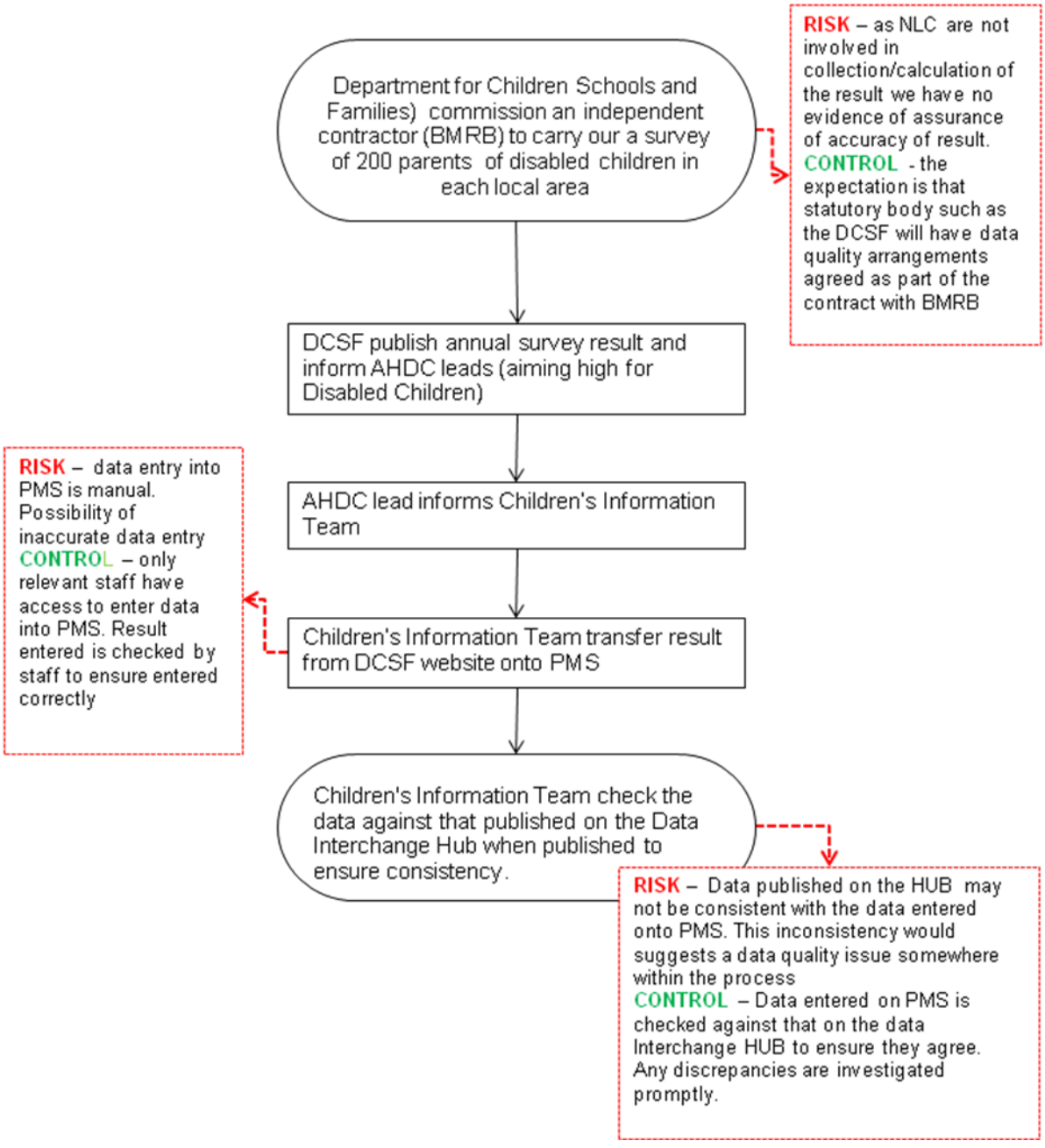
- several tasks/jobs combined into one;
- steps in the process following a natural order;
- work being performed where and when it makes sense and adds value, with limited interfaces, handling points and manual intervention.
- The fewest possible interfaces, handling points and manual intervention.
- the fewest loops back into earlier stages of the process
- The fewest possible activities.

For further information or guidance please contact the Corporate Performance Team

Appendix A (Process Map Guidance)

NI 54 – Services for Disabled Children

This indicator is based on a survey carried out by a private survey firm on behalf of the DCSF. The local authority has no input into the process in any way, and cannot therefore be responsible for the conduct of the process, except when results are published and recorded on PMS



This is a much simplified version of BV215a – rectification of street lighting for illustration purposes ONLY