Report of the Director of Policy and Resources

Decision to be taken after 11 February 2013

NORTH LINCOLNSHIRE COUNCIL

CABINET MEMBER POLICY & RESOURCES

INFORMATION SECURITY POLICY

1. OBJECT AND KEY POINTS IN THIS REPORT

1.1 To consider and approve an updated information security policy (formerly known as the IT security 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 security policy is key to protecting the integrity of our vision.
- An information security policy has been produced to set out the framework and strategic direction for all activities relating to Information Security.

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 an information security policy is a key requirement to ensure we meet our obligations arising through the NHS public health transition arrangements.

2.3 The importance of information security needs to be reinforced across the workforce. This launch of this policy will ensure all staff are made aware of their responsibilities on information security, and therefore ensures they are accountable for their actions.

2.4 The council does significantly more work with other organisations and agencies than ever before. Whilst this is beneficial and supports our

vision, it also opens us up to greater information security risks. This policy sets out a framework and strategic direction for information security and supports greater third party working.

2.5 The benefits of pursuing information security include:

- Minimise the risk of financial damages arising through an information security breach.
- Protect the reputation of the council.
- Increase information security awareness to all staff members through compulsory training.
- Proactively comply with the changing environment for local authorities in relation to obligations enforced by the Information Commissioner.

2.6 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 the legal framework for information security along with clearly defined responsibilities. It also includes arrangements for the following:

- Homeworking/remote working
- Procurement of Services
- Disposals
- Systems and Software
- Information Handling
- Data sharing
- Managing security incidents

2.7 The policy also includes provision for the inclusion of a protective marking scheme, which will be developed during 2013-14. Based on the Government Protective Marking Scheme (GPMS) it will provide a framework for information handling, processing and transmission. The scheme will require the person handling the information to 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

3. OPTIONS FOR CONSIDERATION

3.1 Option 1 – Approve the information security policy

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 information security policy would provide a clear framework for preventing, monitoring and responding to information security breaches. Approving the policy would also ensure the council is complying with the NHS public health transition arrangements.

4.2 Option 2 – Not approving the information security policy could result in a negligent information security breach not being prevented or a fragmented response to a breach as the policy in relation to information security is not clear to all employees. This policy needs to be in place for the end of March 2013 to enable the public health transition to take place.

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

5.1 A training programme has been designed to raise awareness of information security, and this will take varying forms to ensure it reaches all appropriate council employees. Where possible staff will be trained through an e-learning package, whilst those without IT access will have alternative training made available. No extra resources will be needed to cover this as the Policy and Resources directorate will lead and work with other directorates on this.

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.

6.2 The development of this policy goes some way to ensure compliance with the Data Protection Act 1998, Freedom of Information Act 2000 and the Environmental Information Regulations 2004.

7. OUTCOMES OF CONSULTATION

7.1 Consultation has taken place with the council management team, legal services, HR, IT, internal audit, unions and directorate staff as appropriate to develop this policy.

8. RECOMMENDATIONS

8.1 That the cabinet member approves the information security policy

DIRECTOR OF POLICY AND RESOURCES

Civic Centre
Ashby Road
SCUNTHORPE
North Lincolnshire
DN16 1AB
Author: Adam Hopley
Date: 28 January 2013

Background papers used in the preparation of this report:

Integrated Impact Assessment: Information Management Policy (January 2013)

North Lincolnshire Council Information Security Policy (January 2013)

North Lincolnshire Council Information Management Policy (December 2011)

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

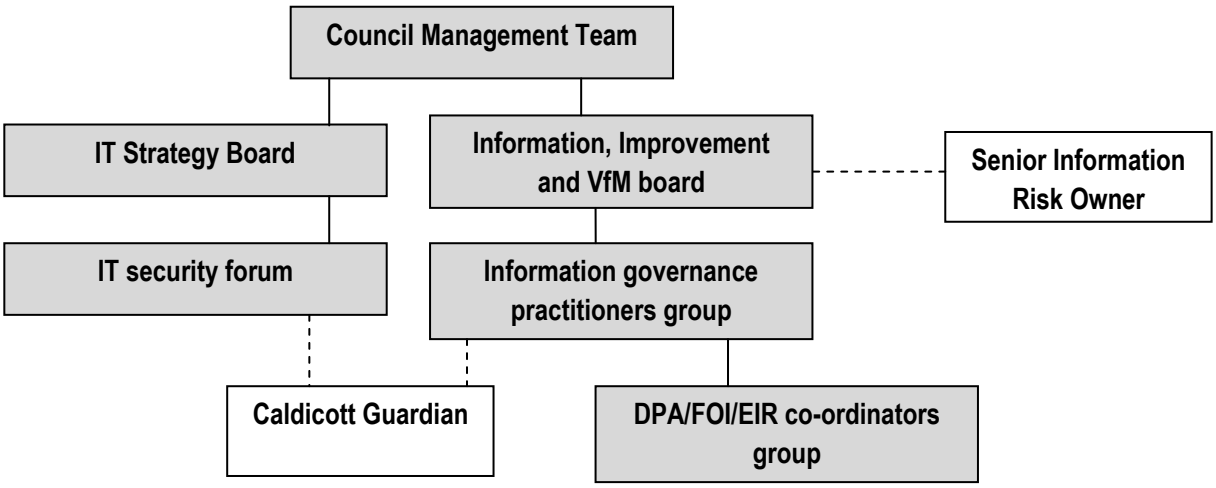
This policy is supported by more detailed policies, standards and procedures. These include but are not limited to the following:

- 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.