Report of the Director of
Policy & Resources

Decision to be taken after
12 November 2012

NORTH LINCOLNSHIRE COUNCIL

POLICY & RESOURCES CABINET MEMBER

INFORMATION MANAGEMENT POLICY UPDATE: DATA BREACH PROCEDURE

1. OBJECT AND KEY POINTS IN THIS REPORT

1.1 To update the council's information management policy to reflect a new procedure for the handling of breaches relating to the Data Protection Act.

- A recent review of the council's Information Management framework identified a need to develop a policy governing the handling of breaches relating to the Data Protection Act
- The Information Commissioner's Office provide guidelines on the handling of DPA breaches
- The information management policy has been updated to recognise the requirements
- The purpose of the policy is to ensure that a standardised management approach is implemented in the event of a data breach

2. BACKGROUND INFORMATION

2.1. Our Information Management Policy is an overarching policy setting out our responsibilities and activities in relation to information management in accordance with specified legislation and professional principles. It provides a framework that enables us to manage our information efficiently. It also promotes the effective management of this information across the organisation, recognising its value as a corporate asset for the delivery of efficient, appropriate, open and transparent services.

2.2. It also sets out to ensure the council complies with the Data Protection Act 1998, Freedom of Information Act 2000, and Environmental information Regulations 2004. It guides the specific operational procedures and activities connected with the implementation of these acts\regulations.

2.3. This framework houses a collection of different policies and from time to time legislation and regulation demand that we update or append new policies.

2.4. In the unlikely event that data is lost or shared inappropriately, whether by the council or contractors/subcontractors working on its behalf, it is vital that appropriate action is taken to minimise any associated risks as soon as possible. Breaches of the DPA can expose the council to fines of up to £0.5m.

2.5. The purpose of the new policy is to ensure that a standardised management approach is taken to the handling of data breaches in line with ICO guidelines.

2.6. The policy contains a Breach Management plan that broadly consists of four elements:

- Containment and Recovery: the Head of Information Management will appoint a team and lead an investigation.

- Assessment of ongoing Risk: the Investigation Team will 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.

- Notification of breach to ICO: after seeking legal advice, the Investigation Team will decide whether anyone should be notified of the breach.

- Evaluation and response: fully review both the causes of the breach and the effectiveness of the response to it, culminating in a report for the council management team (CMT).

3. OPTIONS FOR CONSIDERATION

Option 1: Adopt the new policy

Option 2: Amend or Reject the new policy

4. ANALYSIS OF OPTIONS

4.1 Option 1 is recommended given the requirements recommended by the Information Commissioner.

4.2 The policy is endorsed by the council's Information Management Group.

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

5.1 **Financial**
Breaches of the DPA can expose the council to fines of up to £0.5m.

5.2 **Staffing**
Internal communication methods will be used to notify staff of the requirements of the policy together with dissemination via the information management group

5.3 **Property & IT**
None

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

None

7. OUTCOMES OF CONSULTATION

7.1 Members of the Information Management Group have considered and agreed the policy.

7.2 The Information Management Policy will be updated and re-published on the council's web site.

8. RECOMMENDATION

8.1 That the new information management policy relating to data breach handling is adopted.

DIRECTOR OF POLICY & RESOURCES

Civic Centre
Ashby Road
Scunthorpe
North Lincolnshire
DN16 1AB
Author - C Daly
Date - 11 October 2012

Background Papers used in the preparation of this report:
ICO Guidance
NLC IM Policy
Relevant Legislation

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