Northumberland
County Council

DATA INCIDENT POLICY

DOCUMENT REFERENCE	VERSION	DATE OF THIS VERSION	DATE OF ORIGIN
NCC/IG12	1.0	01/05/2021	09/06/2016

	APPROVED BY	APPROVAL DATE
1	Chief Information Officer	March 2018
2	Information Governance Group/SIRO	May 2022

DATE REVIEWED	REVIEWED BY	APPROVAL DATE	NEXT REVIEW DATE
19 Mar 2018	Data Protection Officer	March 2018	Feb 2020
22 Mar 2018	Caldicott Guardian	March 2018	Feb 2020
01 May 2022	Information Governance Group/SIRO	May 2022	May 2025

Northumberland
County Council

Related Policies

POLICY NAME	POLICY REFERENCE NUMBER	VERSION
Records Management Policy	NCC.IG01	1.3
Data Protection and Confidentiality Policy	NCC.IG02	5.3
Information Security and Transportation, Transfer and Sharing of Data Policy	NCC.IG10	

Amendment History

VERSION	DATE	DESCRIPTION
0.1	09/06/2016	Working draft
1.0	20/03/2018	Amendments to policy in line with General Data Protection Regulation coming into force
2.0	01/05/2021	Updated processes for managing Data Incidents

Northumberland
County Council

1. Scope

1.1 The scope of this Policy applies to the following:

- Northumberland County Council employees and Elected Members
- Agency workers or sub-contractors who work for Northumberland County Council and access NCC data, IT systems or computer networks
- Commercial Suppliers and Organisations processing NCC data who have an obligation to notify the Council of a breach

2. Purpose

2.1 To have a standardised management approach throughout the council when data incidents are reported, or in the event of a serious data breach reportable to the Information Commissioners Office, by having clear policies and procedures in place. Fostering a culture of proactive reporting and logging to maximise the potential for incidents and/or breaches to be identified and addressed.

2.2 Incident management is the process of handling data incidents and data breaches in a controlled way ensuring they are dealt with efficiently, with a consistent approach to ensure that any damage is kept to a minimum and the likelihood of recurrence is reduced by measures taken.

3. Introduction

3.1 Northumberland County Council is responsible for the security and integrity of all information it holds. The Council must protect this information using all means necessary by ensuring at all times that any near miss or actual data incident which could cause damage to the Council's assets and reputation is prevented and/or minimised as well as damage or distress to the data subject.

3.2 A personal data breach can be broadly defined as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed." A data breach is a type of security incident, however, the UK GDPR only applies where there is a breach of personal data. Near misses, are any kind of breach which could have occurred but was prevented by early intervention.

3.3 Examples of Personal Data Breaches.

- Unauthorised access to personal information;
- Unauthorised copying of personal information;
- Unauthorised/incorrect sharing of personal information;
- Unauthorised removal/destruction of personal information;
- Alteration of personal data without permission
- Loss of availability of personal data
- Theft or loss of IT equipment containing personal information.
- Deliberate or accidental action by a Data Controller or Data Processor.

3.4 This policy applies to all types of data incident and near misses. In completing the **Data Incident Form**, it will then be determined whether a data incident or data breach has occurred.

3.5 Data Breaches can be categorised according to the following three information security principles:

3.5.1 **Confidentiality breach**

A confidentiality breach is where there is an unauthorised or accidental disclosure of, or access to, personal data.

Example 1: A database containing personal data relating to children in care is accidentally attached and circulated via email to all foster carers. The carers can then access details of every child in care, including their name, date of birth, address and foster parent's details. The breach has resulted in the accidental disclosure of personal data.

Example 2: An employee sets up a new business providing commercial services to residents. The employee sends themselves a spreadsheet containing residents data held by the County Council, which they intend to use to market their services. This breach was a result of the unauthorised access to, and use of personal data.

Example 3: Letters including personal data are packaged into envelopes. The wrong address is written on the front of the envelope and the recipients receive a letter containing someone else's personal information. This breach has resulted in the accidental disclosure of personal data.

3.5.2 **Integrity Breach**

An integrity breach is where there is an unauthorised or accidental alteration of personal data

Example 1: John Smith contacts the council to update his address. There are multiple John Smith's on the database, the wrong John Smith's address is updated and information is then sent to the wrong address. This breach has resulted in an accidental alteration of personal data.

3.5.3 **Availability Breach**

An availability breach where there is an accidental or unauthorised loss of access to, or destruction of, personal data.

Example 1: An NCC officer uses a notebook to record their client notes. They visit a client and upon leaving, forget to pick up their notebook. The notebook contains a large amount of personal information. This breach has resulted in accidental loss of access to personal data and would also be considered a breach of confidentiality.

Example 2: A member of the team decides to clear out the paper records in the office. They are not familiar of the retention period of the files. They decide to clear space and shred the documents. The documents should have been kept in line with the service retention schedule. This breach has resulted in the accidental destruction of personal data.

4. Reporting Data Incidents

4.1. All potential, suspected or actual data incidents must be reported to the Information Governance Team.

4.2 The individual who discovers or receives a report of a data incident must complete the Council's **Data Incident Form** which can be found on the council's website and staff intranet page - under Information Governance.

4.3.1 This form can be used by internal members of staff who are concerned about a data incident.

4.3.2 All suppliers or organisations processing data on behalf of Northumberland County Council are legally required to notify of a data incident involving Council data.

4.3 If the incident occurs or is discovered outside normal working hours this should be done as soon as practically possible. Data incidents may need to be reported to the Information Commissioner's Office within a 72 hour timeframe, therefore it is important to report all data incidents as soon as possible.

4.4 Details of data incidents can be very sensitive and any sensitive information must be handled with discretion and only disclosed to those who need to know the details.

4.5 Under all normal circumstances employees or others working on behalf of the council must not attempt to deal with a data incident (other than reporting the incident using the **Data Incident Form**) without consulting with the Information Governance Team. However, there will be occasions when immediate action can be taken by individuals to reduce the impact of a data incident ie recall of an email sent to an incorrect recipient / immediate collection of hard copy documentation sent to an incorrect address.

4.6 The Information Governance Team will determine whether a data incident or an actual data breach has occurred and will process this in accordance with the appropriate data incident management plan. Employees must not attempt to conduct their own investigations, unless authorised to do so by the Information Governance team, to ensure evidence is not destroyed.

4.7 The council's Data Protection Officer is ultimately responsible for leading the incident management plan for the data incident in question and making any decisions, in conjunction with the Senior Information Risk Officer (SIRO) about notification of a data breach to the Information Commissioner's Office (ICO) when required to.

5. Data Incident Management Plan

5.1 Breach Management Plan

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

- Containment and recovery.
- Assessment of ongoing risk.
- Notification of breach.
- Evaluation and response.

Northumberland
County Council

5.2 Containment and Recovery

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

5.2.2 Data breaches will require not just an initial response to investigate and contain the situation but also a recovery plan including, where necessary, damage limitation. This will often involve input from specialists across the Council such as IT, HR and legal and in some cases contact with external stakeholders and suppliers

5.2.3 All **Data Incident Forms** are accessible to the Information Governance Team and Data Protection Officer (DPO). The Information Governance Team will consider the data incident reported and discuss this further with the most relevant individuals an appropriate course of action, including practical steps and who should be notified of the data incident, both inside and outside the Council.

5.2.4 Where appropriate, the Data Protection Officer with consult with the Senior Information Risk Owner then there is a requirement to inform the police of a Data Breach.

5.3 Assessment of Ongoing Risk

5.3.1 Following a data breach, it is essential as part of the management plan, that the Head of Service assesses the risks arising from the data breach and if they are likely to reoccur. The Information Governance Team and Data Protection Officer can offer advice and support with this process.

5.3.2 The Head of Service should ascertain whose information was involved in the breach, what led to the breach and what action can be taken to prevent the breach from reoccurring and ensuring any mitigating actions can be implemented immediately.

5.3.3 Examples of Mitigation:

- Notifying/Contacting Recipients
- Retrieval of Information from Recipient
- Informing the Data Subjects
- Removal of Access to Systems
- Review of Internal Procedures/processes
- Re-Training of Staff

5.4 Notification - ICO and Communication to affected Individuals

5.4.1 Every data incident reported to the Information Governance Team will be considered on a case-by-case basis and will be determined whether a data breach has actually occurred.

5.4.2 The Information Governance Team will work with individuals from the affected Service to ensure the most appropriate steps are taken and to ascertain full details of the breach, determine whether the breach is still occurring, recover any losses and limit the damage. Steps might include: -

- Informing Data Subjects that there has been a personal data breach of their information
- Attempting to recover any lost equipment or personal information.
- Shutting down an IT system or remotely wiping lost devices
- Contacting the Communications Team so they can be prepared to handle any press enquiries or to make any press releases.
- The use of backups to restore lost, damaged or stolen information.
- If bank details have been lost/stolen consider contacting banks directly for advice on preventing fraudulent use.
- Making a building secure
- 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

5.4.3 In the event of a personal data breach, the Information Governance Team will assess whether the data breach meets thresholds to be reportable to the Information Commissioners Office within 72 hours. The Information Governance Team will notify the Data Protection Officer if that threshold has been met.

The assessment should consider: -

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

- Whether there has been any media or social media coverage of the data breach

5.4.4 The Data Protection Officer will make the final decision on whether the data breach is likely to result in **high risk** to the rights and freedoms of individuals and if so, they will notify the Senior Information Risk Owner of the breach. An **ICO Personal Data Breach Notification Form** will then be completed and submitted to the ICO within **72 hours** of being made aware of the breach.

5.4.5 When the Council does not notify a breach to the ICO within 72 hours after becoming aware of it, the Council must be able to provide reasons for this delay - to ensure it is justified and not excessive. The timeliness of reporting breaches is therefore an essential aspect of compliance

5.4.6 All Data Breaches will be assessed to determine whether Data Subjects need to be notified of a personal data breach. When notifying individuals, communication must be in clear and plain language, and at least provide:

- A description of the nature of the breach;
- The name and contact details of the Data Protection Officer;
- A description of the likely consequences of the breach; and
- A description of the measures taken or proposed to be taken by the Council to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

5.4.7 Communication to affected individuals is not required under the following conditions;

- If technical and organisational measures have been taken i.e. encryption, or;
- There is discorporate effort involved i.e. if the contact details of the individuals affected is not known or if the individuals cannot be easily identified. In the case of disproportionate effort, data subjects must be informed in an equally effective manner, i.e. public announcement.

5.4.8 The Data Protection Officer and Senior Information Risk Owner will determine whether any further internal investigations are required when assessing serious data breaches that have been reported to the ICO or Police. This may result in further fact-finding investigations. This will involve appointing Senior Managers of the Council to the following positions:

- Lead HR Advisor
- Investigating Officer
- Technical Advisor
- Case Lead

This report will be kept confidential but recommendations detailed in the Final report will be actioned.

Northumberland
County Council

5.5 Review and Evaluation

5.5.1 Once the data breach has been mitigated, data subjects and ICO notified when required, the Information Governance Team will review both the causes of the breach and the effectiveness of the response to it, and will follow up with the applicable services to determine if any further control improvements are required.

5.5.3 The Data Protection Officer will report a summary of the ICO reportable data breach to the Information Governance Board and a summary to the Executive Team.

6. Training and Awareness

6.1 All staff and Members need to be introduced to their basic responsibilities under the UK General Data Protection Regulation in regard to protecting the data we hold and the systems that we use, which includes understanding what is an incident and how to report it. To ensure that they are aware, they will need to complete an annual mandatory training module 'UK General Data Protection Regulation' in addition to reading this policy.

6.2 Some employees will require further training and guidance. Those employees will be identified through their work and initial discussion with their line manager. In these instances, tailored training will be put in place by the Information Governance Team.

6.3 Additional Training will be provided by the Information Governance Team to individuals and service areas where there are regular/frequent data incidents occurring.

6.3 The Data Protection Officer has responsibility to ensure that all levels of the organisation receive appropriate training in the UK General Data Protection Regulation.

7. Compliance

7.1 Any violation of this policy will be investigated and if the cause if found to be wilful disregard or negligence, it may be treated as a disciplinary offence. All disciplinary proceedings are coordinated through the Human Resource Department.

8. Implementation

8.1 This policy is effective immediately.

Northumberland
County Council

9. Monitoring and review

9.1 This policy will be monitored by the Senior Information Risk Officer (SIRO) and Data Protection Officer (DPO) and will be reviewed every three years or where there are changes to legislation.