Northumberland County Council

SECURITY INCIDENT AND DATA BREACH POLICY

DOCUMENT REFERENCE	VERSION	DATE OF THIS VERSION	DATE OF ORIGIN
NCC/IG12	0.2	28/02/2018	09/06/2016

	APPROVED BY	APPROVAL DATE
1	Chief Information Officer	March 2018

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

Northumberland County Council

Related Policies

POLICY NAME	POLICY REFERENCE NUMBER	VERSION
Records Management Policy	NCC.IG01	1.2
Data Protection and Confidentiality Policy	NCC.IG02	5.0
Information Security and Transportation, Transfer and Sharing of Data Policy	NCC.IG10	

Amendment History

VERSION	DATE	DESCRIPTION
0.1	09/06/2016	Working draft
0.2	20/03/2018	Amendments to policy in line with General Data Protection Regulation coming into force

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
- Members of the public may also wish to report a security incident.

2. Purpose

2.1 To have a standardised management approach throughout the council in the event of a serious security incident or data breach 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 incidents and 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 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 is 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 breach is a type of security incident, however, the 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 The difference between a security incident and a personal data breach, in essence, is that whilst all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches. This policy applies to all types of security incident and near misses. In completing the **Security Incident/Security Breach form**, then it will determined which type of breach has occured.

3.4 **Breaches can be categorised according to the following three information security-principles:**

3.4.1 **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. These 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 send 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.

3.4.2 **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 an 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.

3.4.3 **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 Security Incidents and Data Breaches

4.1. This section is about reporting all security incidents and data breaches to the Information Governance Team, classifying the incident and taking appropriate mitigating action.

4.2 The Information Governance Team is made up of the following employees:

- Data Protection Officer
- Records Manager
- Data Protection and Information Governance Officer
- Data Protection and Information Governance Assistant

4.3 The individual who discovers or receives a report of a security incident must complete our **Security Incident/Data Breach Form** which can be found on our website and staff intranet page - under Information Governance.

4.3.1 This form can be used by internal members of staff, a supplier - processing data on behalf of the Council, or a member of the public who is concerned about a breach.

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

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

4.5 The individual should identify into which of the following three categories the incident fits:-

- An actual or suspected data breach.
- An IT security incident that is not a data breach.
- Another type of security incident that puts personal information at risk but is not a data breach.

Appendix A provides further information to assist with categorisation of security incidents and data breaches.

4.6 Details of security 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.

4.7 Under all normal circumstances employees or others working on behalf of the council must not attempt to deal with a security incident (other than reporting the incident using the **Security Incident/Data Breach Form**). Where action needs to be made immediately, this must be passed to the Data Protection Officer or Information Governance Team in the DPO's absence, as soon as possible.

4.8 The Data Protection Officer will determine whether it is a security incident or data breach and will allocate it in accordance with the appropriate management plan. Employees must not attempt to conduct their own investigations, unless authorised to do so, to ensure evidence is not destroyed.

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

4.10 In some circumstances security incidents should also be reported to GovCertUK using the details shown in Appendix C and by following published procedures from these other organisations. This will be determined following submission of your breach form, by the Information Governance Team, in conjunction with NCC IT Design Assurance Officer.

5. Security Incident/Data Breach Management Plan

5.1 Breach Management Plan

5.1.1 The Data Protection Officer will lead all data breach 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.

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 All **Security Incident/Data Breach Forms** will be shared with the Information Governance Team and directed to the Data Protection Officer (DPO). The DPO, or nominated representative in the DPO's absence, will consider the breach and the most appropriate course of action, including practical steps such as who should contact whom, both inside and outside the Council.

5.2.3 In the event of a serious breach an **Incident Response Team** will be brought together as soon as possible following the DPO/nominated representative being made aware of the breach. The Incident Response Team will have 72 hours to investigate whether the breach represents a risk to the Rights and Freedoms of others, and therefore whether it should be reported to the ICO.

5.2.4 The Incident Response Team will include:

- Data Protection Officer (Chair)
- Senior Information Risk Owner (SIRO)
- Principle Lawyer or Head of Legal Services
- Chief Information Officer
- Caldicott Guardian (where the breach compromises the confidentiality of patient and service-user information)
- Head of Communications or nominated representative (where appropriate)
- Head of Internal Audit or nominated representative (where appropriate)

5.2.5 The Data Protection Officer will work with the manager for the service affected and together they will take appropriate steps 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 individuals that they have been affected by a breach
- 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.

5.2.6 The initial investigation should be completed urgently and an **Incident Investigation Report** will be produced by a nominated officer or the Data Protection Officer (depending on the severity of the breach) within 72 hours of the breach being discovered/reported.

5.2.7 The investigation should consider: -

- The type of information or equipment affected
- The category and sensitivity of the information
- How many individuals are affected by the breach? How many records are affected?
- What protections are 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.

Appendix B provides further information about preserving evidence.

5.2.8 The Data Protection Officer will retain a copy of the Incident Investigation Report detailing the nature of the breach, steps to preserve evidence, the assessment of risk/investigation, and the actions taken to mitigate the breach, any notifications made and recommendations for future work/actions. This will be shared with the service manager and summarised in an action plan. The DPO will then support the service manager to oversee and implement the plan.

5.3 Assessment of Ongoing Risk

5.3.1 Following a breach it is essential as part of the management plan, that the manager assess the risks arising from the breach and if they are likely to reoccur. The Data Protection Officer can offer advice and support with process.

5.3.2 The manager 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, including refreshing staff training, and making immediate improvements to processes which are vulnerable to a breach.

5.4 Notification - ICO and Communication to affected Individuals

5.4.1 If the data breach is likely to result in **high risk** to the rights and freedoms of individuals then it is mandatory to notify the ICO without undue delay and within **72 hours** of being made aware of the breach.

5.4.2 Every incident will be considered on a case-by-case basis and the decision to report to the ICO will be determined by carrying out a risk assessment. The Data Protection Officer will assess the risks of each case using the methodology recommended by the ICO, and developed by The European Union Agency for Network and Information Security (ENISA). The methodology gives a score which calculates the severity of a breach using the following formula:

Severity = DPC x EI + CB

Data Processing Context (DPC) - addresses the type of data involved in the breach, together with a number of factors linked to the overall context and use of processing.

Ease of Identification (EI) - Determines how easily the identity of the individual can be deduced from the data involved in the breach

Circumstances of breach (CB) - Addresses the specific circumstances of the breach, which are related to the type of the breach, including mainly the loss of security of the breach data, as well as any involved malicious intent.

Additional points will be added based on the volume of individuals affected - using the following scale:

Additional score	Description of volume of individuals affected
0	Information about 10 or less individuals
1	Information about 11-100 individuals
2	Information about 101-1,000 individuals
3	Information about 1,001 and over individuals

The scores will then be collated and used to determine an overall rating of risk from low to very high. Risks which are high or very high will require notification to the ICO.

SEVERITY RATING ASSESSMENT		
SE < 2	**Low**	Individuals either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spend re-entering information, annoyances, irritations etc)
2 ≤ SE < 3	**Medium**	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments etc)
3 ≤ SE < 4	**High**	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, worsening of health etc)
4 ≤ SE	**Very High**	Individuals may encounter significant, or even irreversible consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death etc)

5.4.3 All high or very high risk incidents must be communicated directly to the affected individuals and without undue delay. 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.

5.4.4 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 dispoporitate 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.

5.4.5 The Data Protection Officer will make the final decision regarding communication to individuals and escalation of an incident to the ICO. These actions must not be taken by anyone else, unless directed to do so by the Data Protection Officer.

5.4.6 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.

5.5 Review and Evaluation

5.5.1 Once the initial after effects of the breach are over the Data Protection Officer should fully review both the causes of the breach and the effectiveness of the response to it, and work with Internal Audit, Senior Information Risk Owner (SIRO), Cauldicott Guardian, or other relevant Officers to determine if any further control improvements are required.

5.5.2 The Data Protection Officer will follow up with a service following a breach, to discuss the causes of the breach and monitor that any necessary changes identified in the breach management plan are implemented in a timely manner.

5.5.3 The Data Protection Officer will report a summary of the incident to the Corporate Leadership Team (CLT) as appropriate.

6. Training and Awareness

6.1 All staff and Members need to be introduced to their basic responsibilities under the 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 in Information Security and 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 Data Protection Officer.

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

9. Monitoring and review

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

10. Useful contacts

Data Protection Officer	Fay Cooper
Caldicott Guardian	Elizabeth Morgan elizabeth.morgan@northumberland.gov.uk
Information Governance Team	informationgovernance@northumberland.gov.uk
IT Design Assurance Officer	Manjeet Bhabra manjeet.bhabra@northumberland.gov.uk
Information Commissioner's Office	www.ico.org.uk

Appendix A: Guidelines for the categorisation of Security Incidents

Actual or Suspected Data Breach

Examples include:-

- Unauthorised access to council information classified as personal or confidential;
- Unauthorised copying of council information;
- Unauthorised removal of council information;
- Use of illegal or unauthorised software or information;
- Fraud or forgery;
- Unauthorised use of another user's profile (to hide user identity);
- Divulging a password to another user;
- Unauthorised access to council offices;
- Theft or loss of IT equipment containing council information.

IT Security Incident (which may include Data Breaches) -

Examples include:-

- IT network attack;
- Denial-of-Service (DoS) Attack;
- Use of viruses or spyware;
- Unauthorised access to the council's IT network and systems;
- Theft of IT equipment;
- Willful damage to council IT equipment or property;
- Unauthorised removal of council property

Other Security Incident (Not a Data Breach) -

Examples include:-

- Power supply failures & fluctuations;
- Terrorist and bomb attacks, including suspicious packages;
- Unauthorised access to council premises;
- Theft of or damage to council property.

Appendix B: Guidelines for Preserving Evidence

Where appropriate the Information Governance Team or Data Protection Officer must follow these steps to preserve evidence: -

- Keep a log of all events showing how evidence was collected, analysed, transported and preserved;
- Where possible mark evidence with the date, time and name of the collector and witnesses;
- If relevant, dump computer contents from memory to a file and take a backup of the file;
- If relevant, make an image (copy) of the computer hard drive(s), which will be used for further analysis to ensure that the evidence on the original system is unharmed;
- If relevant, IT system logs (both current and archived) should be preserved to provide evidence of the incident discovered, as well as any previous incidents.

Northumberland County Council

Appendix C: Guidelines for Reporting Information Security Incidents GovCert UK

GovCertUK provides CESG's CERT function to UK government, assists public sector organisations in the response to computer security incidents and provides advice to reduce exposure to threat.

The Information Governance Team, in conjunction with NCC IT Design Assurance Officer will determine if an incident needs to be reported to GovCertUK.

An incident can be reported to the GovCertUK Incident Response Team who provide a 24 hours 7 days a week operation.

Incidents can be reported in the following ways;
Website: http://www.govcertuk.gov.uk
Telephone: 01242 709311
Fax: 01242 709113
Email for Incidents and alerts: Incidents@govcertuk.gov.uk or govcertuk@cesg.gsi.gov.uk