CORPORATE AND COMMUNITY SERVICES

Data Breaches and Incidents Policy

DECEMBER 2019

North Kesteven
DISTRICT COUNCIL

Date of publication:	April 2018
Reviewed & updated:	December 2019
Next review:	December 2021

Alternative Formats

This document can be made available in large print, braille, audio tape, electronic formats such as CD, or in an alternative language. Our website is ReadSpeaker enabled. For a copy please contact the Corporate Information Team at the Council using the following options:

Phone: 01529 414155 (main switchboard)

Web: www.n-kesteven.gov.uk

Email: equality@n-kesteven.gov.uk

Corporate Information Manager
North Kesteven District Council
Kesteven Street
Sleaford
Lincolnshire
NG34 7EF

Contents

1. Introduction

A data breach is any incident involving the loss of personal information that could have an impact on individuals. The data breach includes electronic, media and paper records and it can also mean inappropriate access to information.

a. Causes

Data protection breaches could be caused by a number of factors. Some examples are:

- Loss or theft of data or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Equipment Failure;
- Human Error;
- Unforeseen circumstances such as fire or flood;
- Hacking;
- Offences where information is obtained by deception.

b. Breach reporting

i. Approach

By adopting a standardised consistent approach, we aim to ensure that breaches and/or incidents are:

- Reported in a timely manner and can be properly investigated
- Are handled appropriately by authorised personnel (namely the DPO)
- Are recorded and documented
- The impact is understood and action taken to prevent further damage
- Data subjects and/or external parties are informed as required
- Are dealt with in a timely manner and are reviewed to identify future improvements.

Throughout the breach management process, records will be kept of what action has been taken and by whom. In addition, a data breach log will be utilised to record this information, including any copies of correspondence.

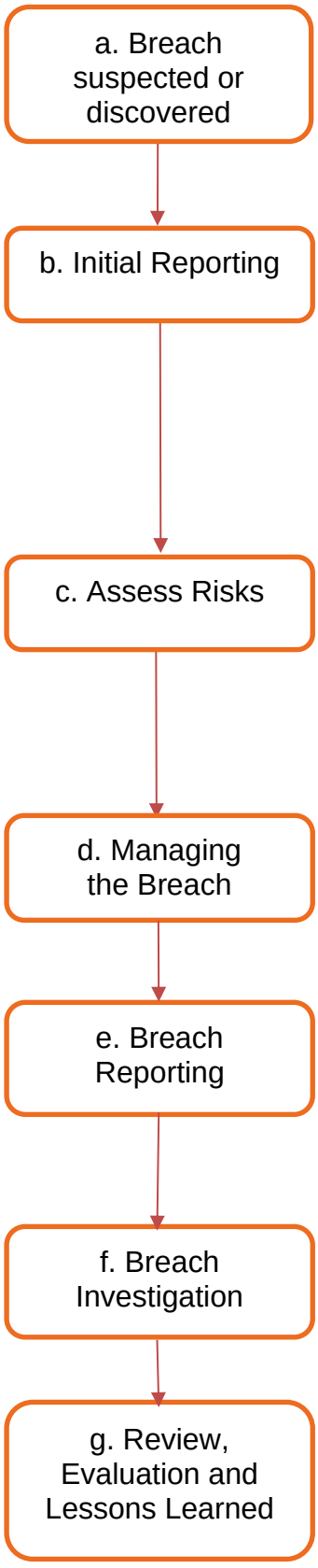
ii. Breach Reporting Obligations on Data Processors

Data processors are required to notify the data controller (the Council) of a personal data breach without undue delay.

iii. Sanctions for Non-Compliance

Failure to comply with breach reporting requirements under the GDPR and DPA will result in regulator scrutiny, negative PR and, possibly, loss of business (dependent on the role of the Division and loss of data). There are also financial penalties, with the standard maximum amount applying, which is 10 million Euros (or equivalent in sterling) or 2% of the total annual worldwide turnover, whichever is higher. The higher maximum amount is 20 million Euros (or equivalent in sterling) or 4% of the total annual worldwide turnover, whichever is the higher.

2. Data Breach Process Summary



- Report immediately to Manager and Data Protection Officer (DPO) by contacting dataprotection@n-kesteven.gov.uk
- If outside of working hours, this should take place as soon as is practically possible

- Manager and DPO to complete 'Breach/Incident Report Form'
- Manager and DPO to determine whether breach still occurring
- If still occurring, steps must be taken immediately to minimise the effect of the breach
- If not still occurring, take no further action and go to 'Assess Risks'

- DPO to review the data protection incident levels and complete the 'Assess Risks' form
- No risk – no further action
- Low, medium or high risks – go to 'Managing the Breach'

- Manager and DPO to recover losses and limit the damage
- Manager and DPO to complete the 'Managing the Breach' form

- DPO to complete this form and undertake actions, including informing the ICO
- DPO to consider notifying affected individuals'
- DPO to consider notifying other organisations, e.g. Police

- DPO to investigate the breach
- All relevant employees to support the investigation

- DPO to review the causes of the breach and effectiveness of response
- Potential remedial action may be required Agreed actions and target dates for completion (and improvement plan if necessary)
- DPO to complete the 'Review and Evaluation' form

3. The Data Breach Process

The seven stages of the data breach process are summarised by the flow chart in Section 2. Detail on the actions required and forms to be completed at each stage is provided below.

a. Breach suspected or discovered

Immediately report the suspected or discovered breach to the Manager and Data Protection Officer (DPO) by contacting dataprotection@n-kesteven.gov.uk.

Examples of data breaches and incidents include:

- Misdirection of emails or correspondence containing personal data;
- Unauthorised access to personal data;
- Theft or loss of papers or electronic media containing personal data;
- Publication of personal data on a website;
- Loss or theft of any Council-owned data storage device, regardless of the data it contains e.g., laptop, iPad, removable hard drive, mobile phone, etc.
- Hacking and data corruption
- Data input errors
- Unescorted visitors in secure areas.

b. Initial Reporting

The person who discovers a breach must inform their Manager and the Data Protection Officer (DPO) immediately. If the breach occurs or is discovered outside normal working hours, this should begin as soon as is practicable. All relevant employees must co-operate promptly with their Manager and DPO to avoid any unnecessary delays, which includes completing the Breach/Incident Report Form at Appendix 3A as quickly as possible. This will also help determine whether a data breach has occurred and the urgency of response required. If in doubt, it is better to report a suspected incident by contacting dataprotection@n-kesteven.gov.uk.

The information in the form will provide key details of the breach/incident, including a description of what happened, when it occurred and any immediate action taken. The DPO will be able to provide advice and assistance when completing the form and, once received, the breach will be logged corporately.

As part of the initial reporting process, the Manager and DPO must ascertain whether the breach is still occurring. If so, steps must be taken immediately to minimise the effect of the breach. An example might be to shut down a system, or to alert relevant employees.

c. Assess Risks

All data and incident breaches must be managed according to their risk, and the 'Data Protection Incident Levels' found in Appendix 3B should be utilised to help determine this. However, an incident level may change once the full facts and impact has been determined, therefore the status of the breach will be kept under review accordingly.

In addition, Appendix 3B provides the line manager with further questions that can be used to assess the risk level, whilst providing further information to the DPO to understand the sensitivity of the data and the number of individuals whose data has been compromised. As above, the DPO will provide guidance and assistance when reviewing the data protection incident level and associated risks.

d. Managing the Breach

If it is concluded that a breach has occurred, the Manager and DPO must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:

- Attempting to recover lost equipment
- Contacting the Council's Contact Centre, Benefits or other relevant Council Departments, so that they are prepared for any enquiries asking for further information
- Contacting the Communications Team so that they can be prepared to handle any press enquiries
- The use of back-ups to restore lost/damaged/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 agencies and employees informed
- Use of backup equipment to restore lost or damaged data or ensuring that employees recognise when someone tries to use stolen data to access accounts
- Where appropriate, inform the police.

The DPO will also contact ICT, particularly if there is an actual or potential security risk arising from an incident involving IT systems or equipment. For example, this could include lost or stolen IT equipment or devices, or unauthorised access to data or systems. In addition, data loss incidents may occur as a result of, or in connection with, major IT incidents (please see the Cyber Resilience Policy, which is available on the corporate website). Appendix 3C will also be completed at this stage, which includes actions, such as, identifying whether the breach has been controlled and determining whether anything can be done to recover losses and limit damage caused.

e. Breach Reporting

Data controllers are required to report a personal data breach to the Information Commissioner's Office (ICO) without undue delay and, where feasible, no later than 72 hours after becoming aware of it, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of data subjects. If a notification is made after the 72 hour period has expired, the Council must explain the reasons for the delay.

As part of the notification to the ICO, this must include:

- A description of the nature of the breach, including, where possible, the categories and approximate number of data subjects and personal data records concerned;
- The name and contact details of the DPO (or alternative contact);
- The likely consequences of the data breach; and
- Measures taken or proposed by the Council to address the breach and/or mitigate its effects.

Where a personal data breach is likely to result in a high risk to the rights and freedoms of a data subject, the Council must communicate the breach to individuals without undue delay. The communication of any data security breach must be handled with care and sensitivity and must describe in clear and plain language the nature of the breach and at least provide the following information:

- The name and contact details of the DPO (or alternative contact);
- The data involved, plus the likely consequences of the data breach
- Advice on what steps they should take, for example, contacting their bank;
- Measures taken or proposed by the Council to address the breach and/or mitigate its effects and how the Council will keep them informed.

However, the DPO and Manager will review whether notification to the data subject is necessary, particularly where any of the following conditions have been met:

- Technical and organisational measures have been applied to the personal data which will render it unintelligible to unauthorised persons (such as encryption);
- The Council has taken steps to ensure the originally high risk is no longer likely to materialise; or
- To notify each individual would involve disproportionate effort, in which case a public communication or other method of information is used which would inform the affected data subjects in a similarly effective manner.

Where a breach is reported to the ICO and not to the data subjects, the ICO may require the Council to notify affected individuals anyway.

Please see Appendix 3D for a more detailed form to be completed with regards to breach reporting.

f. Breach Investigation

In most cases, the next stage would be for the DPO to fully investigate the breach, which will consider the following (of which most will have been documented throughout this process):

- How many people are affected and who (for example, residents, suppliers, tenants)
- Type of data
- Sensitivity of the data
- Potential effect on the individual
- What protections/safeguards are already in place (e.g. encryption)
- What happened to the data
- Whether the data could be put to any illegal or inappropriate use

- Whether there are wider consequences to the breach.

A clear record should be made of the nature of the breach and the actions taken to mitigate it.

The investigation should be completed as soon as possible. A further review of the causes of the breach and recommendations for future improvements can be done once the matter has been resolved.

g. Review, Evaluation and Lessons Learned

The DPO should fully review both the causes of the breach and the effectiveness of the response to it. The breach may highlight remedial action required in relation to procedures, additional training requirements, IT systems and so on. Any agreed actions and target dates for completion will be recorded on Appendix 3E. If systemic or ongoing problems are identified, then an improvement action plan must be drawn up.

It should be noted that there could be the recommendation of the pursuance of the relevant disciplinary procedure for employees where the circumstances of a particular incident make it appropriate to do so. Any such recommendation will be made to the Human Resources Team.

4. Policy Review

This Policy will be formally reviewed on an annual basis to ensure it continues to be relevant and current. In some circumstances it may be necessary to review this Policy more frequently in response to specific events.

5. List of accompanying data breach forms

Appendix 3A – Breach-Incident Initial Report Form
Appendix 3B – Assess Risks
Appendix 3C – Managing the Breach
Appendix 3D – Breach Reporting
Appendix 3E – Review and Evaluation

North Kesteven
DISTRICT COUNCIL

District Council Offices, Kesteven Street, Sleaford, Lincolnshire NG34 7EF
Telephone Number: (01529) 414155
180912-JA2