Data Security Incident Management Procedure

This procedure explains the actions Southend-on-Sea City Council will take in the event of personal data appearing to have been lost, stolen or otherwise wrongly disclosed.

If you think you have just discovered or been responsible for a breach of personal data, a quick guide of what to do is given at Appendix 1. Please go straight to this and take the action shown. You do not at this point need to read the rest of this procedure as the most important thing is that you act immediately. This is the case even if you are not sure of all the facts now.

The Information Rights Support Service has 72 hours from the discovery of the breach to decide whether we need to make a formal disclosure to the Information Commissioner, so it is important that there is no delay in reporting.

Author: Valerie Smith
Version: 8
Review date: May 2025

Introduction

1.1. Southend on Sea City Council (the Council) holds personal information about its customers, clients and staff. This can range from low level information to very sensitive information about people's lives.

1.2. We all have an obligation to keep people's personal information safe, both under the law[1] and because it is the right thing to do.

1.3. Sometimes however things go wrong and there is a data security incident (often referred to as a 'breach') or the potential for one is identified.

1.4. A data security incident is where information about a person has been or could have been:

- Lost
- Stolen
- Disclosed to someone it should not have been
- Accessed by someone who should not have done
- Damaged, or destroyed when it should not have been
- Wrongly altered

1.5. Examples of an incident or breach are:

- The loss or theft of data held on equipment, such as a laptop or memory stick
- Staff having access to systems they do not need for their job role
- Equipment failure leading to loss of data
- Human error in dealing with personal information, such as sending a letter or e-mail to the wrong person
- A fire or flood which destroys records
- A hacking attack on the Council's ICT systems
- 'Blagging' offences where information is given to someone who pretends to be someone else

- The following are the policies and procedures which explain how personal information should be managed to avoid the above happening:

    - Data Protection Policy
    - Records Management Policy
    - Document Retention and Disposal Policy
    - Confidential Waste Policy

[1] Data Protection Act 2018, UK General Data Protection Regulation and others

- Acceptable Use Policy (ICT systems including remote working)
- IT Disposal Procedure

2. Purpose

2.1. This procedure explains what officers of the Council will do when a data security incident has happened or the potential for an incident is identified.

2.2. Its purpose is to ensure a standardised approach throughout the council and that any data security incidents are managed in a structured and controlled way so that:

- Potential damage or harm to the person(s) concerned is kept to a minimum
- Action is taken speedily, consistently and in accordance with legislation
- Trends, patterns and wider issues are identified and lessons learned to reduce the likelihood of an incident happening again.

3. Scope

3.1. This procedure applies to all users of the Council's information, data, information systems and the Council's property portfolio (its physical buildings). It applies not only to staff and members but also to service providers and consultants and encompasses data, information, software, systems and paper documents.

4. Roles and Responsibilities

4.1. Details of the roles and responsibilities of specialist officers, teams and groups are outlined in Appendix 2.

Incident Management

4.2. The important elements to the management of a data security incident are:

- Reporting the security incident/breach
- Containment and recovery
- Assessment of the on-going risk
- Notification of the breach
- Evaluation and response

4.3. The procedure for the Council's management of data security incidents is set by the Senior Information Risk Officer (SIRO). It is designed to meet NHS Information Governance guidelines and the Information Commissioner's breach management guidelines.

4.4. The investigation of incidents is led by the Data Protection Officer[2].

5. Reporting the security incident or breach

5.1. Incidents or breaches must be reported to the Data Protection Officer or their team as soon as they are identified. Anyone in the organisation can make a report. It should not be delayed because the exact circumstances are not known. If it is unclear whether a report should be made, advice should be sought from the Data Protection Officer or Information Rights Support Service. Contact details can be found on the intranet.

5.2. It is important that the report is made as soon as the problem is identified. This is because the Data Protection Officer must tell the Information Commissioner about some breaches and a decision has to be made within 72 hours of the breach being identified. Failure to do so could result in financial penalties for the Council, damage to our reputation and a loss of public trust.

5.3. There is a form on the intranet to prompt the information which the Data Protection Officer will need to know. At the initial stage the form simply seeks to capture what has happened and the seriousness of the incident.

5.4. Do not delay reporting if you do not know all the information requested. Help with completion of the report can be provided on request from the Data Protection Officer.

5.5. It is good practice to inform your line manager of the situation but do not delay reporting because senior officers are absent or unavailable.

6. Containment and Recovery

6.1. The Data Protection Officer will assign an officer to lead on the investigation of the incident. They will work with those concerned to identify:

- Who in the organisation needs to be advised of the incident
- Who will need to assist in containing the incident
- Whether anything can be done to recover lost information

---

[2] Reference to the Data Protection Officer throughout includes specialist staff under their direction

- Whether the potential for damage can be limited
- Whether the Police need to be involved

6.2. It is the responsibility of the Director or Group Manager of the service concerned to take whatever steps are judged necessary to contain any breach and recover information where appropriate.

6.3. It is a co-operative process and, depending where investigations lead, could involve multiple parts of the organisation. In some cases, it will be necessary to make contact with external stakeholders and suppliers.

6.4. It is particularly important that this stage of the process is given top priority by all concerned as it is the best opportunity to limit the potential harm to the individual(s) whose personal information may have been put at risk.

7. Assessment of the on-going risk

7.1. To help decide on appropriate containment measures, the Data Protection Officer will assess the risks which may be associated with the incident. Usually, the most important factor will be an assessment of the potential adverse consequences for individuals, how serious or substantial these are and how likely they are to happen.

7.2. Considerations will include, but are not limited to:

- What type of data is involved?
- How sensitive is it?
- Are there any protections in place such as encryption?
- Could the data be used for harmful purposes?
- What could the data tell a third party about the individual?
- How many individuals' personal data is affected?
- Who are the individuals whose data has been breached and what harm could come to those individuals?
- Are there wider consequences to consider such as a risk to public health or loss of public confidence in an important service you provide?
- Is advice from a third party such as a bank needed about risk reduction options?

7.3. The urgency and nature of response will be in proportion to the assessed risk.

8. Notification of the breach to the affected individual

8.1. The Data Protection Officer will, in co-operation with others[3], assess whether it is appropriate to notify the affected individual of a data security breach.

8.2. The Information Commissioner advises that notification is not an end in itself and should have a clear purpose, such as to enable individuals who may have been affected to act on the information provided to reduce risks, for example by cancelling a credit card or changing a password.

8.3. If it is assessed that there is a high risk to the rights and freedoms of an affected person, they must be told of the breach urgently.

8.4. This will apply when there is likely to be:

- A significant detrimental effect on the individual
- Discrimination
- Damage to the individual's reputation
- Financial loss
- Any other significant economic or social disadvantage

8.5. The decision whether to notify will be made in accordance with relevant legislation and guidance.

10. Notification of the breach to the Information Commissioner

10.1. The Data Protection Officer will, in co-operation with others, assess whether it is appropriate to notify the Information Commissioner of a data security breach.

10.2. The Information Commissioner advises that it is mandatory to report a breach to their office if it is likely to result in a risk to people's rights and freedoms. If this is unlikely, there is no need to make a report. The threshold therefore depends on the risk posed to those involved.

10.3. The test suggested by the Information Commissioner is whether, if the risk was unaddressed, it would have a significant detrimental effect on the individual(s) concerned. For example:

- Discrimination
- Damage to reputation
- Financial loss
- Loss of confidentiality

---

[3] In particular, the Senior Information Risk Owner, Privacy Officer and Caldicott Guardian as appropriate

- Other significant economic or social disadvantage (such as identity theft)

10.4. The SIRO will authorise and monitor notifications to the Information Commissioner. The decision whether to notify will be made in accordance with relevant legislation and guidance.

11. Notification within the Council

11.1. Depending on the type of information involved and the assessed level of risk, the Data Protection Officer will notify a breach to:

- The Senior Information Risk Owner
- The Privacy Officer
- The Caldicott Guardian
- The Director/Group Manager of the service area where the breach occurred
- The Chief Executive and Deputy Chief Executive
- The Strategic Communications Manager

12. Notification of other bodies

12.1. It may be necessary to notify additional regulatory bodies or other parties that a breach has occurred. This includes but is not limited to:

- The NHS Information Governance Team
- The police - especially if there is concern for the safety of the individual(s) concerned
- Insurers, professional bodies, bank or credit card companies who can assist in reducing the risk of financial loss
- Trade unions
- Relevant partner agencies

12.2. The Data Protection Officer will, in co-operation with others, assess whether it is appropriate to notify the other bodies of a data security breach, taking advice as necessary.

13. Evaluation and response

13.1. It is important not only to investigate the cause of an incident or breach but also how well we responded to it. The Data Protection Officer will maintain a record of security incidents and breaches and will periodically review the response to reported incidents to monitor the effectiveness of this procedure and will initiate any necessary amendment or clarification to it.

13.2. Where investigation of an incident identifies the need for staff training in data protection matters, this will be arranged. This may be generic training or a tailored response depending on the need.

13.3. Where a breach is shown to have been caused by officer negligence, appropriate disciplinary action may need to be taken. In this event, the Data Protection Officer will alert the relevant officer in the HR department who will advise the responsible line manager concerning the relevant Council procedures to be followed.

13.4. Where investigation of an incident or breach identifies systemic problems, these will be highlighted by the Data Protection Officer and responsibility for resolution will be passed to an individual within the relevant department.

13.5. Where there is dispute over who should be responsible for the necessary action which cannot be resolved in another way, the matter will be referred to the Governance Board for their intervention.

13.6. When remedial steps are put in place these should be reported to the Data Protection Officer as they will form part of the evidence for the Council's compliance with data protection legislation.

13.7. A summary of data security incidents, breaches and the learning from them will be regularly presented to meetings of the Caldicott Board, the Governance Board (or their subsidiary). Information will also be presented in the annual SIRO report to Members.

Appendix 1

Immediate action in the event of a data security incident or breach

1. Do not attempt to deal with a security incident on your own

2. Tell your direct line manager what has happened and /or tell someone in your area of at least Group Manager Level - but - don't delay if they cannot be reached

3. Tell the Information Rights Support Service straight away (or get your line manager to do so) – it doesn't matter if you don't yet know exactly what has happened

4. A form to prompt the information the Information Rights Support Service will need is on the intranet.

5. If there is an immediate opportunity to get the information back – take it (for example if someone has contacted you to say they have received something they shouldn't, ask for it back)

6. Be discreet – don't cause alarm by discussing potentially sensitive matters in an open area or with people who do not need to know at this stage

7. If in doubt – ask for advice from the Data Protection Officer or Information Rights Support Service before taking any action.

Version Control

Date	Version	Reason	Owner	Author
May 2018	Version 5	Review of guidance and reflection of GDPR requirements	SIRO	Valerie Smith
January 2020	Version 6	Review and minor updates	SIRO	Valerie Smith
May 2022	Version 7	Review and minor updates. Updated to link to new intranet and to reflect City status.	SIRO	Valerie Smith
May 2023	Version 8	Review and minor updates to reflect amended information governance structure	SIRO	Valerie Smith (review by Karen Finn)

Purpose:	To provide advice and guidance for the Management of Data Security Incidents and Breaches
Status:	Final
Date:	May 2023
To be reviewed by:	May 2025
Governance	Governance Board