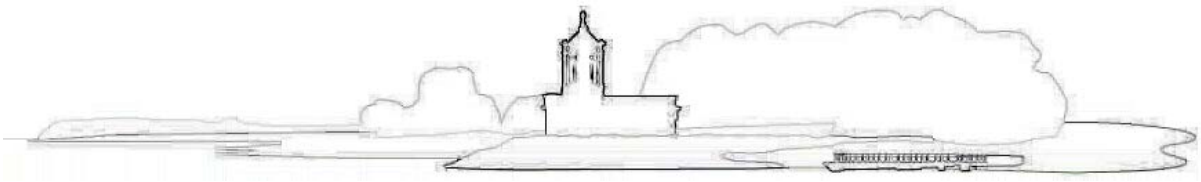
Rutland County Council

DATA INCIDENT RESPONSE POLICY

Version & Policy Number	Version two
Guardian	Data Protection Officer
Date Produced	April 2024
Next Review Date	June 2025

Approved by Cabinet	June 2024



Summary of document

This Policy provides a clear framework in which Members and Officers should operate in the event of a data incident. This Policy should be read in conjunction with other policies and procedures that support the Council's commitment to information governance.

Contents

		Page
1.0	Policy Statement	4
2.0	Breach Management	5
3.0	Monitoring and Review	8
4.0	Contacts	8
	Appendix 1	10
	Appendix 2	14

DATA INCIDENT RESPONSE POLICY

1.1. Policy Statement

Rutland County Council holds personal and special data. Every care is taken to protect personal data and to avoid a data breach. In the event of a data incident, it is vital that appropriate action is taken to minimise any associated risk as soon as possible.

1.2. Purpose

This Policy sets out the procedure to be followed by Members and Officers if a data incident occurs.

1.3. Scope

This Policy applies to all personal and special data held by Rutland County Council (see below).

1.4. Legal Context

The United Kingdom General Data Protection Regulations (UK GDPR) makes provision for the regulation of the processing (use) of information relating to individuals, including the obtaining, holding, use or disclosure of such information.

Principle 6 of the UK GDPR states that organisations which process personal data must "process in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures".

1.4.1. Data

Data means information which applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that contains pseudonyms.

1.4.2. Personal Data

Personal data is data which relates to a living individual who can be identified directly or indirectly by reference to an identifier. A wide range of personal identifiers constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

1.4.3. Special/Sensitive Personal Data

The UK GDPR refers to sensitive personal data as “special categories of personal data” (Article 9 of the UK GDPR).

(a) the racial or ethnic origin of the data subject,
(b) his/her political opinions,
(c) his/her religious beliefs or other beliefs of a similar nature,
(d) whether he/she is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
(e) his/her physical or mental health or condition,
(f) his/her sexual life,
(g) genetic data,
(h) biometric data

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (Article 10 of the UK GDPR).

1.5. Types of Breach

Data protection breaches could be caused by several factors. Some examples are (this list is not definitive):

- 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
- Access by an unauthorised third party;
- Deliberate or accidental action (or inaction) by a controller or processor;
- Sending personal data to an incorrect recipient;
- Alteration of personal data without permission; and

2. Breach Management

A data breach must be reported by the individual who is responsible for or becomes aware of a data breach, to their line manager and the Data Protection Officer (DPO) using the Data Incident Report Form. The DPO will appoint the Information Governance Coordinator (IGC) or another officer to investigate the breach. The Line Manager will determine with the investigator the reason(s) for the breach and measures necessary to remedy the breach and/or prevent a recurrence.

2.1. Containment and Recovery

The Information Governance Coordinator will coordinate with departmental managers to:

- Establish if the breach is ongoing and take immediate action to stop the breach and to minimise the impact and effect of the breach;
- Establish who needs to be made aware of the breach and inform them of what they are expected to do to assist in the containment exercise;
- Establish whether there is anything the Council can do to recover any losses and limit the damage the breach can cause;

- Instigate the recovery of physical equipment, where appropriate;
- As far as is practicably possible, ensure that Council staff recognise and take action to avoid anyone trying to use the lost or stolen data to access accounts;
- Inform the police, where appropriate;
- Inform the banks/building societies and card providers if appropriate: and
- Inform the Communications Team to enable a press statement to be prepared, if necessary.

If the breach occurs or is discovered outside normal working hours, the investigation and notification of relevant officers should begin as soon as is practicable.

Records must be kept of all actions taken in line with Rutland County Councils Retention and Records Management Policy. The DPO is responsible for collating all records.

2.2. Assessment of an Ongoing Breach

The nature of the breach will determine what steps are necessary in addition to immediate containment. This will be done by an assessment of the risks associated with the breach. This risk assessment will be undertaken by the officer responsible for the breach and the IGC.

The most important aspect is an assessment of potential adverse consequences for the subject(s) of the data breach, how serious or substantial these are and how likely they are to happen. This will be based on:

- What type of data is involved.
- The sensitivity of the data.
- If data has been lost or stolen, whether there are any protections in place such as encryption.
- What has happened to the data.
- What the data could reveal about the individual.
- Whether many individuals' personal data is affected by the breach.
- Who data subjects are
- What potential harm could result.

2.3. Notification of the Breach

The DPO shall determine who will be notified, the information the notification will contain and how they will be notified. In determining the extent of the notification, the following should be considered (this is not an exhaustive list, and each breach must be assessed on its own circumstances):

- Which individuals and/or groups need to be notified.
- Are there any dangers of 'over notifying.
- Any contractual or operational requirements.
- The regulatory bodies which require notification.
- Can notification help the Council to meet its security obligations in the 6 data protection principles
- Can notification help the subject(s) of the data breach mitigate any consequences.
- The number of people affected.
- How serious the consequences are.
- What information can be shared in the notification.

2.3.1 Determining Serious Breaches

The presumption is that all breaches are 'serious' breaches unless the facts of the breach indicate otherwise.

The DPO must determine with the Senior Information Risk Owner (SIRO) if the breach is a serious breach that needs to be notified to the Information Commissioner's Office (ICO). This must be done without undue delay and where feasible no later than 72 hours after the breach occurring.

To establish the seriousness of a breach the following must be considered:

- The potential harm to the data subject from the breach, including any distress the data subject may suffer due to the breach.
- The volume of the data involved.
- The sensitivity of the data involved.
- How widely has the data been shared.

Serious breaches should be notified to the ICO, and the notification should include details of:

- The type of information and number of records
- The circumstances of the loss / release / corruption
- Actions taken to minimise / mitigate the effect on affected individuals.
- How the breach is being investigated.
- Whether any other regulatory body has been informed and their response
- Action taken to prevent reoccurrence
- Any other information that may assist the ICO in making an assessment

2.4. Evaluation and Response

Once the breach has been dealt with the Information Governance Coordinator should evaluate and report to the DPO on:

- the effectiveness of the Council's response to the breach.

- Whether the breach was caused in whole or part by systemic and ongoing problems.
- Where the Council's response to the breach was hampered by inadequate policies or a lack of a clear allocation of responsibility then any response must review and update these policies and lines responsibility accordingly.

The evaluation must consider, although not limited to:

- Ensuring individuals know what personal data is held and where and how it is stored.
- Establishing where the biggest risks lie.
- Ensuring that where data is shared, either internally to the Council or externally, the method of transmission is secure and that only relevant data is shared or disclosed.
- Identifying weak points in existing security measures.

- Monitoring staff awareness of data security issues and looking to fill any gaps through training or tailored advice.

2.5 Employment Considerations

This Policy should be read in conjunction with the Data Protection Policy and ICT Security Policy and the Code of Conduct.

Monitoring and Review

This Policy shall be reviewed every 12 months after implementation.

3.1. Implementation

This protocol was implemented on August 2014.

4.0. Contacts

Senior Information Risk Owner (SIRO)	Angela Wakefield
Data Protection Officer (DPO)	Sarah Khawaja
Information Governance Coordinator (IGC)	Dave Cousens

Email: dataprotection@rutland.gov.uk
Tel: 01572 758265