Draft
Data Breach Management Policy 2026

Version 2.0 – April 2026
Next review date: April 2027

Table of Contents

1. Purpose of this document 3
2. Scope and applicability 3
3. Data breaches defined 4
4. Management of data breaches 4
4.1 Immediate steps to be taken by staff 4
4.2 Breach management by the Information & Engagement Team 5
4.2a Containment and recovery 5-6
4.2b Assessment of risk 6
4.2c Notification of the breach 6
4.2d Evaluation and response 7
5. Section 170 Offences, Data Protection Act 7
6. Security incidents 8
7. Third party data processors 8

1. Purpose of this document

This document sets out the data breach management policy and forms part of the Council's Information Governance Policy Framework. The policy aims to ensure that Bolsover District Council reacts appropriately to any actual or suspected breaches of data protection.

The UK General Data Protection Regulation (UK GDPR) Article 5 states that data should be processed 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 ('integrity and confidentiality').

The Council is required to report certain types of personal data breaches to the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach. The Council must report incidents where there is a risk to people's rights and freedoms; this means that there are potential negative consequences for individuals because of a breach.

In practice, this means that the Council must have appropriate security to prevent the personal data we process being accidentally or deliberately compromised. This includes having the right physical and technical security, backed up by robust policies and procedures and well-trained and reliable staff. It also means that the organisation should be ready to respond to any threat to or breach of information security swiftly and effectively and have procedures in place to support that.

2. Scope and applicability

This policy is applicable to Council employees, Councillors, temporary and agency staff and contractors working for and on behalf of the Council and any organisations processing data on the Council's behalf.

It covers all data that is processed by the Council, i.e. all data that is obtained, held or stored, used, shared, retained or destroyed by the Council, and any data processed by a third-party organisation on behalf of the Council (i.e. under a contract).

It covers data in all formats and on all types of media, including paper-based information and documents, digital and electronic information, whether held on the Council's network, at off-site storage, a portable device, in the cloud or in transit.

This policy does not set out the Council's approach when responding to security incidents because of technical failures and/or cyberattacks. This can be found in the Council's **Joint Information and Cyber Security Policy (April 2024)**.

3. Data breaches defined

A personal data breach is a breach of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. This includes breaches that are the result of both accidental and deliberate actions, and it is more than simply 'losing' personal data.

Broadly speaking, where the confidentiality, integrity or availability of personal data has been affected a security incident has occurred.

Examples of data breaches include:

- IT equipment containing personal data being lost or stolen.
- Paper files being lost or stolen.
- Sending data to an incorrect recipient.
- Deliberate action where data taken without authorisation.
- Deleting data before it has reached its retention date.
- Altering personal data without authorisation.

In certain circumstances, the Council has a requirement to report the incident to the ICO within 72 hours.

4. Management of data breaches

Recital 87 of the UK GDPR states that organisations must quickly establish whether a personal data breach has occurred and take steps to address any breach which includes reporting to the ICO if required. Therefore, it is essential that that all breaches are reported to the Information and Engagement (I&E) team as soon as possible.

It is the responsibility of all members of the organisation, including those working on our behalf, to be aware of what constitutes a data breach and the action that needs to be taken in the event of a breach.

Following a data breach, the Council will take steps to contain the breach which includes ensuring that the right people and organisations are notified as soon as possible. Staff have a responsibility to report breaches as they become aware so that the Council can proactively manage the incident.

4.1 Immediate steps to be taken by staff

On becoming aware of a data breach, staff must:

►Report the breach via the following link: https://www.bolsover.gov.uk/data-protection-cctv-and-foi/report-a-data-breach
►Inform their line manager of the breach.
►Comply with any instruction/s from the I&E team.

4.2 Breach management by the I&E team

On receipt of a data breach report, the I&E team will work with the relevant service area to complete the security incident checklist. Following this initial assessment, the I&E team will determine whether the breach should be categorised as 'near miss', low risk or high risk.

The I&E team will work with the service area to contain the incident as far as possible. Immediate rectification actions to mitigate the incident will be provided to the reporting officer, such as asking an incorrect recipient to delete an email beyond retrieval.

The I&E team will escalate incidents to the Data Protection Officer (DPO) or Deputy Data Protection Officer (DDPO) as appropriate. The I&E team is responsible for leading the review of all data protection incidents and will work with the relevant service areas to identify:

■What personal data has been compromised.
■Whether personal data has been inappropriately accessed.
■How the incident can be contained (limiting or restricting further impact of the incident).
■The risk of harm or distress to individuals whose data has been compromised (the data subjects).
■If and/or how data subjects will be told, or 'notified' of the incident.
■How the incident occurred.
■Any weaknesses in the Council's processes, procedures, organisational or technical controls which may have led or contributed to the incident.
■What mitigating actions or controls are required to increase resilience, to prevent or reduce the likelihood or a reoccurrence, or to reduce the impact of any reoccurrence.

The I&E team maintain a register of all breaches and provide details on the number of data breaches and near misses to the SLT. Additionally, the I&E team provide details on the number of serious incidents that have been reported to the ICO as part of the Council's assurance statements.

For all incidents escalated to the DPO/DDPO (i.e. all except near misses), the following approach will be adopted.

4.2.a Containment and recovery

✓The DPO/DDPO shall be alerted to the breach immediately.
✓Any steps to prevent any further breach of the data will be implemented.
✓The DPO/DDPO will immediately notify the SIRO, relevant director and service manager. *Where an incident is very high risk, the Chief Executive Officer will also be notified.*

✓If known from the initial assessment, the DPO/DDPO will provide a recommendation on notification to the ICO and where necessary, will involve the SIRO.
✓The I&E team will alert the Communications team to ensure any media attention can be proactively managed.
✓The I&E team will ensure that Legal Services are notified of serious incidents who will manage any legal action taken against the Council because of a serious incident.
✓The I&E team will convene a meeting with the relevant service managers to review the incident and assess the risk against individuals.
✓The I&E team will identify whether any other organisations have been affected and notify them accordingly.
✓For breaches involving other governmental bodies such as DWP or NHS, further notification will be required as set out below.

4.2.b Assessment of risk

The I&E team will carry out an initial assessment of the risk to the rights and freedoms of individuals and agree the risk level (near miss, low or high). Where necessary, a formal likelihood-versus-impact assessment will be conducted with the relevant service area.

The assessment will always consider the potential impact on individuals' rights and freedoms and the likelihood of that impact occurring. A breach must be reported to the ICO if it is likely to result in a risk to individuals' rights and freedoms (even if the overall risk is assessed as low).

Notification to individuals is required only where the risk is high. The I&E team will work with the service area to carry out the risk assessment based on the following criteria:

■ The type of breach – this may affect the level of risk to individuals.
■ The nature, sensitivity and volume of personal data – the more sensitive the data, the higher the risk of harm (context will always be considered).
■ Ease of identification – encrypted or pseudonymised data reduces the likelihood of identification.
■ Risk of harm to the individuals – physical harm, theft, fraud, psychological distress, humiliation or damage to reputation.
■ Vulnerability of the individuals – for example, children or other vulnerable groups.
■ Number of individuals affected – generally the higher the number, the greater the impact (context will always be taken into consideration).

4.2.c Notification of the breach

The Information Commissioner's Office (ICO)

Where the risk assessment identifies that the breach is likely to result in a risk to the rights and freedoms of individuals, the DPO/DDPO will recommend to the SIRO that the breach is reported to the ICO. The Council will report without

undue delay and, where feasible, not later than 72 hours of becoming aware of the breach. Only breaches assessed as unlikely to result in any risk to individuals' rights and freedoms are exempt from notification (this decision must be documented).

Department of Work and Pensions

In cases where it is identified that DWP information has been breached, the I&E team will report the breach to the DWP's DPO.

NHS Digital

All incidents (regardless of severity) involving Health and Social Care data must be reported by the I&E team via the NHS Data Security and Protection Incident Reporting tool. This will report incidents to the NHS Digital, Department of Health, ICO and other regulators.

Individuals

Where it has been identified that individuals should be notified of the breach, correspondence will be sent via the accountable Director for the affected service. The DPO/DDPO will provide support with wording for the letters/emails and any recommended protective steps for individuals.

4.2.d Evaluation and response

The I&E team will document all findings in a report, which will include:

■Details of the breach and how it occurred.
■The risk assessment of the incident and subsequent recommendation of reporting to the ICO.
■Risk assessment and recommendations around notification of individuals.
■Outline training completed by members of staff.
■Recommendations and actions that should be taken to mitigate the breach occurring in the future.

The report will be shared with the SIRO, CEO, and relevant Director.

5. Section 170 Offences, Data Protection Act

Section 170 (s170) of the Data Protection Act 2018 sets out a criminal offence in relation to individuals unlawfully obtaining personal data. Specifically, s170 states that it is a criminal offence for an individual to:

■Knowingly or recklessly obtain, disclose or procure personal data without the consent of the data controller.
■Sell data that was obtained unlawfully.
■Recklessly retain personal data – even if it was obtained lawfully – without the consent of the data controller.

If it is suspected that a member of staff has committed a s170 offence, the breach must be reported in the usual manner and investigated by the I&E team.

If a I&E-led investigation identifies that a member of staff has likely committed a s170 offence under the Data Protection Act 2018, the above process will be followed to assess the risk, and the following will also occur:

►HR to be notified immediately so that advice can be taken on disciplinary action.
►The ICO to be contacted to seek their advice on notification.
►Whether the breach is so serious that a report needs to be made to the Police.

In serious cases where s170 offences have occurred, the I&E team will report the matter to the ICO who will determine whether they wish to prosecute the individual for the offence.

6. Security incidents

The ICT team will lead on the technical response for any cyberattack that has affected Council systems.

For serious breaches that are a result of a technical failure, an incident manager will be identified by the SIRO. The incident manager will be responsible for overseeing the Council's response to the incident, ensuring that tasks are completed and will liaise with I&E team as required.

7. Third party data processors

Third party data processors who process personal data must be made aware of their responsibilities and their obligations to the Data Controller (the Council), and how to report a data breach or security incident.

Contracts with third parties who process personal data on behalf of the Council must include robust clauses to ensure that personal data is processed in accordance with the UK GDPR. The contract between the Council and the contractor provides the legal basis for the data processing, the categories of data being processed and sets out information security management procedures. Any breaches of data caused by a third-party processor must be reported in accordance with this policy.

For further information about Bolsover District Council's compliance with data protection law, please email GDPR@bolsover.gov.uk.