

Data Breach Management Policy

Version 2.1, December 2024

Revision history

Date	Version	Summary of action	Author
Mar – Jul 2009	0.1 – 0.4	Policy creation	Jeremy Tuck
September 2011	0.5	Policy reviewed and updated. Escalation process added	Sinead Mulready
July 2013	0.6	Annual policy review	Sinead Mulready
April 2016	1.0	Annual policy review and procedure extracted from policy	Leila Ridley
February 2017	1.2	Annual policy review	Janice Abraham
May 2018	1.3	Annual policy review and preparation for GDPR	Shona Nicolson
April 2019	1.4	Annual policy review	Reece Watson
December 2020	1.5	Annual policy review: updated to comply with accessibility requirements and Brexit	Reece Watson
December 2021	1.6	Annual Review: Updated to remove reference to Information Governance Lead Group and update Information Asset Owner definition.	Reece Watson
December 2023	1.7	Updated as part of policy framework review	Leila Ridley
February 2024	2.0	Published	Leila Ridley
December 2024	2.1	Annual policy review	Leila Ridley

Table of Contents

1. Purpose of this document	2
2. Scope and applicability	3
3. Data breaches defined	3
4. Management of data breaches	4
4.1 Immediate steps to be taken by staff	4
4.2 Breach management by the IDG team	4
4.2.1 Containment and recovery	5
4.2.2 Assessment of risk	6
4.2.3 Notification of the breach	6
4.2.4 Evaluation and response	7
5. Section 170 Offences, Data Protection Act	8
6. Security incidents	8
7. Breaches that occur out of hours	8
8. Third party data processors	9

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 Islington 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 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. Details of how these incidents are managed are set out in the Cyber Security Incident Process.

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.
- Using a third party to manage or store personal data without a contract in place.

In certain circumstances, the council has a requirement to report the incident to the Information Commissioner's Office 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 Information Commissioner's Office (ICO) if required. Therefore, it is essential that all breaches are reported to the Information and Digital Governance (IDG) 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 this link:
<https://islingtonportal.icasework.com/form?Type=Breach&db=islington>.
- Inform their manager of the breach.
- Comply with any direction from the IDG team.

4.2 Breach management by the IDG team

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

The IDG team will work with the service area to contain the incident so far as possible. Immediate rectification actions to mitigate the incident will be provided to the reporting officer, such as asking an incorrect recipient to an email to delete it.

The IDG team will escalate incidents to the Data Protection Officer as appropriate. The IDG 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 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 IDG team maintain a register of all breaches and provide details on the number of data breaches and near misses to the IG Board. Additionally, the IDG team provide details on the number of serious incidents that have been reported to the ICO to CMT and as part of the council's Annual Assurance statement.

Where incidents are deemed to be high risk, the following approach will be adopted.

4.2.1 Containment and recovery

- The Data Protection Officer (DPO) shall be alerted to the breach immediately.
- Any steps to prevent any further breach of the data will be implemented.
- The DPO will immediately notify the SIRO, Monitoring Officer, relevant corporate director and Information Asset Owner (IAO). Where an incident is very high risk, the Chief Executive Officer will also be notified.
- If known from the initial assessment, the DPO (or the Data Protection Manager in the DPO's absence) will provide a recommendation on notification to the ICO and individuals to the SIRO.
- The IDG team will alert the Communications team to ensure any media attention can be proactively managed.
- The IDG Team will ensure that Legal Services are notified of serious incidents who will manage any legal action taken against the council as a result of a serious incident.
- The IDG team will convene a meeting with the relevant IAO and managers to review the incident and assess the risk against individuals.

- The IDG team will identify whether any other organisations have been affected and notify them accordingly.
- For breaches involving DWP or NHS data further notification will be required which is set out below.

4.2.2 Assessment of risk

The IDG team will carry out an initial assessment of the risk and meet with the DPO to agree the risk level. Where necessary the IDG team and the DPO will work with the relevant service area to conduct a risk assessment using likelihood vs impact.

The IDG team will always give consideration the potential impact on the rights and freedoms of individuals as well as the likelihood of this occurring. Where the consequences and risk of harm is higher it is likely that the threshold will be met for reporting to the ICO and/or notifying the individuals.

The IDG 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 it is likely that there will be a higher risk of harm to the individual, however context will always be considered.
- Ease of identification – an assessment of how easy it would be to identify an individual from the data. Encrypted and pseudonymised data will reduce the likelihood of the person being identified.
- Risk of harm on the individuals – what is the harm that an individual could face and how severe is this, for example is the person at risk of physical harm, theft, fraud, psychological distress, humiliation or damage to reputation.
- How vulnerable is the individual – is the data about children or other vulnerable individuals who may be at greater risk.
- How many individuals have been affected – generally the higher the number affected the greater the impact, however the context will always be taken into consideration.

4.2.3 Notification of the breach

4.3.1 The Information Commissioner's Office

Where the assessment identifies that there is a high risk to the rights and freedoms of individuals the DPO will recommend to the SIRO (or the deputy SIRO) that the breach should be reported to the ICO. On authorisation the DPO (or a member of their team) will report the breach to the ICO.

The council will endeavour to report serious breaches to the ICO within 72 hours.

4.3.2 Department of Work and Pensions

In cases where it is identified that DWP information has been breached, the IDG team will report the breach to the DWP.

4.3.3 NHS Digital

All incidents (regardless of severity) involving Health and Social Care data must be reported by the IDG team via NHS Data Security and Protection Incident Reporting tool (the incident reporting tool for the NHS in England). This will report incidents to the NHS Digital, Department of Health, ICO and other regulators. All incidents should be reported, not just serious incidents, as they all need to be logged and assessed.

4.3.4 Department for Education

All incidents that affect data extracts received from the DfE, where the council is operating as a processor to the DfE as Controller, must be reported to the DfE Data Protection Officer. Further information regarding the data extracts in scope and the contact details for the DfE Data Protection Officer may be found in the Agreement for the Supply of Data Extracts (Controller to Processor) between the Department for Education and the London Borough of Islington. Copies of the agreement are held by both Children's Services and the IDG team.

4.3.5 Individuals

Where it has been identified that individuals should be notified of the breach, it is expected that correspondence is sent via the accountable IAO or Corporate Director for the affected service. The IDG team will provide support with wording for the letters and/or emails as well as any steps recommended for individuals to protect themselves following a breach.

4.2.4 Evaluation and response

The IDG team will document all findings in a report, this 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, Monitoring Officer, relevant Corporate Director and IAO. In cases where the breach is very serious or high risk, the report will also be sent to the Chief Executive Officer.

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 IDG team.

If an IDG-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, but the following will also occur:

- HR to be notified immediately so that advice can be taken by their line manager 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 IDG 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 Cybersecurity 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 IDG team as required.

7. Breaches that occur out of hours

If data breach occurs out of office hours, the matter must be reported to Emergency planning. If the matter is serious, Emergency planning will pick this up and:

- Contact the relevant personnel in Digital Services by phone to escalate the matter.
- If not already alerted, Digital Services colleagues will alert the Data Protection Officer to ensure that any notification to the ICO can still be made within the 72 hours.

- The DPO will alert the SIRO.
- The on-call Emergency Planning Officer (EPO) will inform the on-call media officer and on-call Director.
- The EPO will provide media and senior officers with the single point of contact from Digital Services for the incident.
- The on-call Director will take advice from the DPO to brief the Chief Executive, relevant Corporate Director and Members.

8. 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 Islington Council's compliance with data protection law, please contact us: dp@islington.gov.uk