ISLINGTON

Islington Council
Information Security Incident Policy

A council-wide information security policy

Version 1.7

May 2019

Revision History

Date	Version	Reason for change	Author
4 Mar 09	0.1	First draft	Jeremy Tuck
8 May 09	0.2	Incorporated comments following TSG review	Jeremy Tuck
1 July 09	0.3	Comments incorporated from Louise Round, HR, the CoCo Programme Board, the TIM Board. Incorporated the relevant Children's Services Contact Point requirements	Jeremy Tuck
30 July 09	0.4	Incorporated Incident flow diagram and new incident categories into the appendices. Removed named references to the Network Security Advisor	Jeremy Tuck
7 Sept 11	0.5	Policy reviewed and updated. Escalation process added (Section 6.6)	Sinead Mulready
20 June 2013	0.7	Annual review	Sinead Mulready
5 July 2013	0.7.1	Following review with Shona Nicolson and Adrian Gorst	Sinead Mulready
1 March 2016	1.1	Following review with Shona Nicolson and Adrian Gorst	Leila Ridley
14 April 2016	1.2	Extraction of procedure from policy.	Leila Ridley
Feb 2017	DRAFT V1.3	Annual Review	Janice Abraham
Jan 2018	Draft v 1.5	Review in advance of GDPR	Shona Nicolson
May 2018	1.6	Approved and published	Shona Nicolson
April 2019	1.7	Annual Review	Reece Watson

Review schedule

This policy will be reviewed for relevance and accuracy by the Data Protection Officer annually

Table of Contents

1 OVERVIEW

This document sets out the Information Security Incident Management Policy for Islington Council. The policy aims to ensure that Islington Council reacts appropriately to any actual or suspected security incidents relating to information systems and data.

The EU General Data Protection Regulation (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 as a result 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.

This policy should be read in conjunction with the Information Security Incident Procedures.

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, a portable device, cloud or in transit.

3 DATA SECURITY INCIDENTS DEFINED

A data security incident is any event or error which compromises the 'personally identifiable data' held by the council and is considered to be a breach of the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. This data may identify staff, residents or customers. The GPDR requires the council to have 'appropriate organisational and technical measures in place' to protect such data. A data security incident may involve personally identifiable data being:

- Lost
- Stolen
- Disclosed publically
- Inappropriately accessed by council staff

- Inappropriately accessed by third parties

4 IT SECURITY INCIDENTS DEFINED

An IT Security Incident is an adverse event that has caused or has the potential to cause damage to an organisation's assets, reputation and / or personnel. Incident management is concerned with intrusion, compromise and misuse of information and information resources, and the continuity of critical information systems and processes.

An Information Security Incident includes, but is not restricted to, the following:

- The loss or theft of data or information.
- The transfer of data or information to those who are not entitled to receive that information.
- Attempts (either failed or successful) to gain unauthorised access to data or information storage or a computer system.
- Changes to information or data or system hardware, firmware, or software characteristics without the council's knowledge, instruction, or consent.
- Unwanted disruption or denial of service to a system.
- The unauthorised use of a system for the processing or storage of data by any person.
- An information security threat is where a weakness or vulnerability has been identified that could have led to an information security event.

5 PRINCIPLES OF THIS POLICY

5.1 All staff

- The security of data is the responsibility of every individual working for the council and all staff need to protect data at all times.
- All users must understand and adopt this policy and are responsible for ensuring the safety and security of the council's data and the information that they use.
- All incidents must be reported via ICT Helpme, using the Security Incident Category.
- All incidents must be reported as quickly as possible. In certain circumstances the council has a requirement to report the incident to the Information Commissioner's Office within 72 hours.
- All incidents involving **Health and Social Care data must be reported by the IG 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.
- Any information security weaknesses or 'near misses' should be reported too. The sooner we know about them; the sooner they can be addressed to prevent an actual breach.
- For serious technical security incidents that occur 'out of hour's' (after 5pm on weekdays or any time on the weekend or a bank holiday), the incident **must** be reported to Emergency Planning on 0207 354 0282.
- All staff should be vigilant for viruses, phishing attempts or spam email. If in doubt, staff should report the incident via ICTHelpme and discontinue use of the equipment until verified by Digital Services.

5.2 Information Governance Team

- The Information Governance (IG) Team will triage security incidents in line with the security incident procedure, working with the relevant service area to complete the security incident checklist.
- The IG team will work with the service area to contain the incident so far as possible.
- The IG team will escalate incidents to the Data Protection Officer as appropriate. The IG 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 IG team will record all information relevant to the incident in the Data Security Incident Register for that year.

5.3 Data Protection Officer

The Data Protection Officer is responsible for:

- Providing advice to the Senior Information Risk Owner (SIRO) as to when the ICO and data subjects should be notified, based on the severity of the incident and provide guidance on how this should be done.
- Liaising with the ICO over the reporting and management of the incident if required.
- Leading the review of serious data breaches and ensuring that a full investigation is undertaken.
- Monitoring compliance with this policy and ensuring continuous improvement.

5.4 Network Security

Network security team will lead on the technical response for any breach that has affected council systems.

5.5 Incident Manager

For serious incidents of a technical nature, 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 the Data Protection Officer as required.

5.6 Emergency Planning

Emergency planning will pick up serious incidents where they occur out of hours. For serious technical security incidents, Emergency Planning will contact the relevant personnel in Digital Services by phone to escalate the matter. 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 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 brief the Chief Executive, relevant Corporate Director and Members.

5.7 Communications

The Information Governance Team will ensure that the Communications Team is made aware of serious incidents to ensure any media attention can be proactively managed.

5.8 Legal

The Information Governance Team will ensure that Legal Services are notified of serious incidents. Legal Services will manage any legal action taken against the Council as a result of a serious incident.

5.9 The Senior Information Risk Owner

The Corporate Director of Resources is the Council's SIRO. The SIRO will be involved in any security incidents, which may meet the threshold for reporting to Data Subjects, ICO or other external bodies and will be responsible for the decision on whether to notify, taking advice from the Data Protection Officer.

Where the SIRO is unavailable and the DPO considers the threshold to report to the ICO is met, the decision can be taken by the Director of Law & Governance (who acts as the Deputy SIRO) or the Chief Executive.

5.10 Information Asset Owners

Information Asset Owners are responsible for the Confidentiality, Integrity and Availability of their Information Assets and for ensuring they have appropriate local procedures and controls in place to protect their data. Additionally, they are responsible for ensuring they have service business continuity plans in place in the event of loss of data availability.

5.11 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 an information 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 General Data Protection Regulation and UK Data Protection Act 2018. 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.

5.12 Information Governance Working Group

The Information Governance Working Group (IGWG) is chaired by the Head of Information Governance and Data Protection Officer and is made up of Information Governance Leads from each of the directorates. The IGWG is responsible for reviewing the nature and frequency of security incidents and of making recommendations to improve training, policy and process

to try and prevent reoccurrences. The IGWG monitors and delivers on actions set out in the IGWG action plan to ensure continued compliance with legislation.

5.13 Corporate Governance Group

This council-wide policy will be reviewed and signed off by the Corporate Governance Group (CGG), chaired by the Corporate Director of Resources, who is also the Council's SIRO. Information Security is included in the CGG terms of reference. The CCG reports directly into the Corporate Management Board (CMB).

CGG are also responsible for reviewing the nature/frequency of security incidents and making recommendations to improve training, policy and process to try and prevent reoccurrences. CGG receive updates on the progress against agreed actions to support the delivery of the Information Governance Strategy and any data protection audits that have taken place.

6 POLICY COMPLIANCE

The Data Protection Officer will monitor compliance with this policy.

If any employee is found to have breached this policy, they may be subject to the Council's disciplinary procedures, up to and including termination of employment. Other users may have their contract terminated immediately.

If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s). If you do not understand the implications of this policy or how it may apply to you, please seek advice from the Data Protection Officer (DP@islington.gov.uk)

7 RISK MANAGEMENT

Risk management for Islington Council is set out in our Risk Management Policy.

8 GOVERNANCE & REVIEW

This policy and the commitment to information security is subject to continuous, systematic review and improvement. This policy will be governed by the Corporate Governance Group (CGG), chaired by the Corporate Director of Resources, who is also the council's Senior Information Risk Owner.

The CGG has a clear terms of reference and reports directly into the Corporate Management Board.

This policy will be reviewed annually by the Data Protection Officer and will be reviewed by the Data Security Working Group and Approved by the Corporate Governance Group.

9 POLICY SIGN OFF

Name	Role	Signature	Date Signed
Nikki Beardmore	**Interim Corporate Director of Resources and SIRO**		
Peter Fehler	**Director of Law & Governance**		
Leila Ridley	**Head of Information Governance & Data Protection Officer**		
Jon Cumming	**Interim Chief Digital and Information Officer**		
Duncan Harris	**Head of Cyber Security**		