ISLINGTON

Islington Information Security Risk Framework

A council-wide information policy

Version 0.7
January 2015

Contacts
If you need any further information about this document or any clarity about the contents of the document, please contact: Sinead Mulready (Data Security Manager).

Revision History

Date	Version	Reason for change	Author
11 June 2012	0.1	First draft	Sinead Mulready
02 Aug 2012	0.2	Comments incorporated following consultation to CAB and the DSWG	Jeremy Tuck
11 Aug 2012	0.3	Further comments incorporated following input from Paul Beard and Sinead Mulready.	Jeremy Tuck
1.12.2012	0.4	Approved by Corporate Management Board	Sinead Mulready
21.6.2013	0.5	Annual Policy review	Sinead Mulready
October 2014	0.6	Annual Policy review and following updated corporate risk management policy	Sinead Mulready
January 2015	0.7	Following review by DSWG and corporate Risk management	Sinead Mulready

TABLE OF CONTENTS

1. Applying the Policy

This document sets out the methods by which Islington Council will provide assurance of how Information Security risks are being managed and how the Information Risk Register will be populated and monitored. This document should be read in conjunction with the council's ICT Policies, the Data Protection Policy and the Information Governance Policy

2. Background

Islington's approach to Risk and Opportunity Management (http://izzi/council/aboutcouncil/performance-policy/policy/Corporate-Governance/Pages/20100125-Risk-Management.aspx) sets out the framework adopted by the Council for managing risk and recording details of any opportunities that may arise from the successful management of risk. This policy sets out specifically how the council manages risks relating to information management, data protection and security.

The council needs to collect and use certain types of information about its staff, residents, customers and clients in order to carry out its functions, but in doing so needs to ensure that it does this in accordance with the requirements of the Data Protection Act 1998 and, in particular, to note that Section 7 of the Data Protection Act 1998 states that appropriate measures must be undertaken to ensure the security of personal data.

The council therefore needs to have a framework to ensure that when new processes, services, systems and other information assets are introduced that the implementation does not result in an adverse impact on information quality or a breach of information security, confidentiality or data protection requirements. This framework sets out a mechanism and behaviours to ensure that information security, confidentiality, protection and quality is considered and that any known risks are identified and addressed.

3. Applying the Policy

3. 1. The council must have documented information policies

The council has documented policies and will review these and update these on an annual basis. These policies should be comprehensive and the contents of these policies need to be formally disseminated to all staff. Where, flowing from the implementation of these policies, there are known risks to the council's abilities to adhere to the principles of these policies, these should be documented as risks, which should then be managed, mitigated and addressed.

3. 2. The council must maintain an Information Risk Register

The council will maintain a documented Information Risk Register (IRR) that will record the identified risk, the departmental responsibility, the impact and likelihood of the risk, and the owner of actions to mitigate the risk. Information risks will be captured in the following ways:

- Risks identified through any new systems introduced
- Risks identified through formal projects
- Outcomes of data audits
- Risks identified and discussed at the Technical Design Authority
- Issues highlighted through the weekly ICT Change Control Board
- Issues raised at the Data Security Working Group
- Issues raised in data protection and security training sessions
- ICT Incident management (eg security incidents and near misses
- Any other issues identied by the Data Security Manager and Information Compliance Manager

Changes not captured through these methods must be notified to the Data Security Manager by logging a request on the ICT Help Me system, under 'Information Risk'.

3. 3. The Information Risk register will be updated by the Data Security Manager

The Data Security Manager will be responsible for updating the Information Risk Register following input from the above boards, groups and processes.

3. 4. Vulnerabilities giving rise to breaches and near misses must update the risk register

All security incidents must be recorded on the council's ICT Help Me system as part of the Incident Management Policy. This includes data breaches and incidents raised relating to Data Protection Act issues. This is the process by which direct issues and risks can be raised by the organization. The Data Security Manager will take responsibility for ensuring that risks and issues raised in this way are recorded on the Information Risk Register, where appropriate.

3. 5. The council must review risks where any changes are introduced

When the council implements new or changed systems, procedures or contracts, or moves of premises, these could affect the way information is stored, processed and shared. Where any changes are planned, it is important that risks to the security of information are recorded and monitored, that the risk is mitigated or accepted, and that a named individual is responsible for these decisions.

Changes in the way personally identifiable data is collected, stored or processed should be reviewed by use of a Privacy Impact Assessment, which should be used to identify potential risks.

The council's Privacy Impact Assessment template and guidance is available on the intranet: http://izzi/council/aboutcouncil/performance-policy/policy/data-security/Pages/Privacy-Impact-Assessments.aspx

All ICT or new system development must firstly be reviewed and approved by the Technical Design Authority, or by the Digital Services Management Team. All new projects, including ICT or capital projects must prepare a risk register. Any new risks that are considered of such a nature that they may impact corporate information risk should should be submitted to the Data Security Manager, who will then review these and where appropriate update the Information Risk Register.

3. 6. The council must identify information risks that arise through IT changes

Changes in IT systems and applications affect the way that data is accessed and stored by the council, and it is important that information risk is understood and captured as part of these changes.

The Technical Design Authority works as a reference board to provide advice and make recommendations about new ICT projects and new changes to systems. This board, therefore, is often aware of risks that may exist on a technical level. Where the TDA identifies information security risk it must ensure that these risks are referred to the Data Security Manager, who will assess the risk and record them on the Information Risk Register where appropriate.

The ICT Change Control Board meets regularly (usually weekly) to review proposed changes to existing / live systems that are either being introduced or modified. As part of this process risks are often highlighted, either when changes are approved or refused. Where the ICT Change Control Board identifies Information Security risks it must ensure that these risks are referred to the Data Security Manager to record on the Information Risk Register where appropriate.

3. 7. The Data Security Working Group must identify and record risks

The Data Security Working Group meets to review and discuss data security issues, with specific overview of information training, policies and security incidents. Through review and discussion of these areas, risks are identified. Where the Data Security Working Group identifies risk it must ensure that these risks are referred to the Data Security Manager to record on the Information Risk Register where appropriate. All risks identified and discussed at this group must be disseminated to service areas by the representing member of the board.

3. 8. Risks identified by staff during training should be recorded

It is often during staff training that local or service security risks are identified and these are often quite specific. Where such risks are identified these need to be recorded onto the Information Risk Register, where appropriate. This should be done by trainers providing information to the Data Security Manager.

3. 9. All *ad hoc* risks identified must be recorded where appropriate

All other appropriate issues that are identified should be recorded on the Information Risk Register or raised through one of the processes mentioned above. These will be assessed on a case by case basis by the Data Security Manager, who will record them.

3. 10. Risks will be rated in line with the council's corporate risk assessment criteria

The council has corporate risk assessment criteria, which require that each risk be rated against its impact and likelihood, giving rise to a numerical rating.

Score	Risk level
1-6	Low
8-12	Medium
15-16	Medium - high
18-30	High

3. 11. The Information Risk register will be reviewed regularly

Review by Data Security Working Group
The information risk register will be reviewed quarterly at meetings of the Data Security Working Group, which will:

a) Qualify and state these risks so that these are clear to the council
b) Review the impact and likelihood of existing risks
c) Agree actions to mitigate and address risks
d) Undertake actions to address these risks
e) Monitor the implementation of actions
f) Review the efficacy of agreed actions
g) Decide and Agree on the closure of risks
h) Revew the need to escalate medium risks to the Corporate Governance Group

Review by Digital Services Management Team

Digital Services maintains a departmental risk register which captures risks related to ICT projects, network security and asset management. These are areas which may impact or affect information risk.

The Digital Services Management team and the Data Security Manager meet on a monthly basis to review both the Information Risk Register and the Digital Services Risk Register, to ensure that risks identified through one are shared with the other as appropriate.

3. 12. Escalation of Information Risks

The Data Security Manager will provide an annual report to the Corporate Governance Group on the Information Risk Register.

The Corporate Risk Manager will be invited to the Data Security Working Group twice a year to provide further review and scrutiny of the information risk register.

Risks with a rating of 15 or above will be escalated on an *ad hoc* basis to the Senior Infomration Risk Owner at point of identification.

Risks with a rating of 8 – 12 will be highlighted to CGG as agreed by the Data Security Working Group.

3. 13. Responding to Risks

The Corporate Governance Group will determine the course of action, mitigation and ownership of the information risks identified by the various groups. The Board will agree actions to mitigate and address these risks and thereafter decide which risks should be accepted by the council or escalated to the council's Corporate Management Board.

4. Governance, approval and review

4. 1. All staff must comply with this policy

All employees are expected to serve the council and implement its policies to the highest standards, as described in the Code of Conduct. If any user is found to have breached this policy, they may be subject to the council's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in the prosecution of the offender(s). Any staff member who wants to understand the implications of this policy or how it may apply must seek advice from the ICT Performance and Assurance Team.

4. 2. Corporate Governance Group

This policy framework and the commitment to security management is subject to continuous, systematic review and improvement. This council-wide technology policy will be governed by the Corporate Governance Group (CGG), chaired by the Director of Finance, 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.

4. 3. Formal approval, adoption and review

This policy will be formally signed off by the Corporate Management Board. The Data Security Manager will lead an annual review of all ICT Security Policies.