Harlow Council

Working together for Harlow

HARLOW COUNCIL
Corporate Information Security Policy

Document Information

Policy Author(s):	**Declan White and EOLP**	Document Version No:	**5.2**
Approved and authorised:		Document Version Date:	**11/09/2014**
Date authorised:		Document Type:	**Policy**
Service	**Finance**	Department	**ICT**

1. Introduction

Information resources are vital to Harlow Council in the delivery of services to residents, businesses and visitors. Their availability, integrity, security and confidentiality are essential to maintain service levels, legal compliance and the public image and perception of Harlow Council.

It is important that service users are able to trust Harlow Council to act appropriately when obtaining and holding information and when using the Council's facilities. It is also important that information owned by other organisations made available to Harlow Council under secondary disclosure agreements is also treated appropriately by Harlow Council.

Any Council that uses or provides information resources has a responsibility to maintain, safeguard them, and comply with the laws governing the processing and use of information and communications technology.

The Chief Executive of Harlow Council has ultimate responsibility and endorses the adoption and implementation of this Corporate Information Security Policy. Delegated responsibilities are set out in section 6 and rest with the Information Security Management Group and the Senior ICT Manager with regard to the maintenance and review of the Policy, Conditions of Acceptable Use and the Personal Commitment Statement as well as local policies.

This Policy is designed to provide an appropriate level of protection to the information for which Harlow Council is responsible. Supporting this Policy is a set of information security technical controls which form the minimum standard that a partner organisation has to comply with. Individual organisations can strengthen these policies through their local policies and procedures, but cannot weaken them.

It is unacceptable for Harlow Council information resources to be used to perform unethical or unlawful acts.

The key aspects of this Policy and all associated policies have been developed in accordance with the British Standard for Information security BS7799 – 3:2006 which is harmonised with ISO/IEC 27001:2005.

This Corporate Information Security Policy is supported by further policies, procedures, standards and guidelines. In addition to this Policy, users who are granted access to information owned by other organisations will be subject to the Policy requirements of the information owners. Details of these policies will be provided before access is granted.

This Policy was developed by the Essex On-Line Partnership and enhanced by Harlow Council.

2. Information Security Framework

This document forms the Information Security Framework for the Council along with any associated policies, procedures and documents

3. Objectives

The objective of the Corporate Information Security Policy is to ensure that:

a. All users are aware of the Policy and associated legal and regulatory requirements and of their responsibilities in relation to information security.
b. All Harlow Council property including equipment and information are appropriately protected.
c. The availability, integrity and confidentiality of Harlow Council information is maintained.
d. A high level of awareness exists of the need to comply with information security measures.
e. To prevent unauthorised access to software and information.
f. To reduce the risk of the misuse of email services.
g. To protect the network and its' resources from unauthorised access.
h. To provide guidance on handling information of each classification in different circumstances and locations including creation, modification or processing, storage, communication, retention and deletion, disposal or destruction.
i. To manage unwanted incidents such as virus infections, deliberate intrusion and attempted information theft.
j. To prevent unauthorised access, damage and interference to business premises, Information and Information Technology.

4. Scope of policy

The scope of this Policy is for any employee, Councillor, agency worker, third party organisation or other authorised personnel.

5. Legal and regulatory obligations

Harlow Council will comply with all relevant legislation affecting the use of information and communication technology. All users will be made aware of and comply with current legislation as they may be held personally responsible for any breach.

A list of key legislation and regulations, with a brief description of each, and a reference to who in the organisation can provide further information can be found in Appendix A.

6. Roles and Responsibilities

- **Chief Executive Officer (CEO)**

The CEO is ultimately responsible for ensuring that all information is appropriately protected.

- **Information Security Management Group**

This Policy has been written by the Essex On-Line Partnership and supplemented by the Council, additional policies, procedures and standards are produced by the Information Security Management Group. The Information Security Management Group is responsible for reviews and approval of security policies, which are reviewed and re-issued each year. The Information Security Group consists of the Head of Finance, the Senior ICT Manager, the Corporate Information Manager. It is also responsible for approving and overseeing all information security related projects and initiatives. Harlow Council's Senior Information Risk Owner (SIRO) is the Head of Finance who ensures the accountability of the policies, procedures and standards.

- **Information Security Officer**

This role is fulfilled by the Senior ICT Manager who is responsible for the day to day management of information security activities, and for responding to information security incidents.

- **SIRO**

The SIRO **must** provide written judgement of the security and use of the business assets at least annually to support the audit process.

The Local Government Association (LGA) guidance and best practice suggests that the SIRO:-

a) Is the officer who is ultimately accountable for the assurance of information security at the Council
b) Champions information security at executive management team level
c) Owns the Corporate Information Security Policy
d) Provides an annual statement of the security of information assets (as part of the audit process)
e) Receives strategic information risk management training at least once a year

The SIRO is not intended to be a new post but a defined set of responsibilities for an existing 'board-level' post. It is not concerned solely with IT, but takes a broader view of our information assets as a whole, in any form.

The SIRO role at Harlow Council is held by the Head of Finance.

- **Risk Manager**

The Risk Manager is responsible for the evaluation of the Council's exposure to risk and controlling these exposures through such means as mitigation, avoidance, management or transference. This role is held by the Senior ICT Manager.

- **Information Owners**

The role of the Information Owners is to understand what information is held and in what form, how it is added and removed, who has access, and why. The Information Owners will normally be Managers within Council departments that use and manage the information on a daily basis. They are tasked with ensuring the best use is made of information, and receive and respond to request

They are responsible for:

a) Assessing the risks to the information and data for which they are responsible in accordance with Harlow Council Risk Management Methodology.

b) Defining the appropriate protection of their information taking into consideration the sensitivity and value of the information.

- **Heads of Service and Line Managers**

Are responsible for:

a) Ensuring that their employees are fully conversant with this Policy and all associated, policies, standards, procedures, guidelines and relevant legislation, and are aware of the consequences of non-compliance.

b) Developing procedures, processes and practices which comply with this Policy for use in their service areas.

c) Ensuring that all external agents and third parties defined in the scope of this Policy are aware of their requirement to comply.

d) Ensuring that when requesting or authorising access for their staff, they comply with the standards and procedures defined by the Information Owners.

e) Notifying the Information Security Officer, Senior ICT Manager through the IT Service Desk, of any suspected or actual breaches or perceived weaknesses of information security.

- **Employees**

Are responsible for:

a) Ensuring that they conduct their business in accordance with this Policy and all applicable supporting policies.

b) Familiarising themselves with this Policy, and all applicable supporting policies, procedures, standards and guidelines.

Employees responsible for management of third parties must ensure that the third parties are contractually obliged to comply with this Policy.

- **Users of systems and information**

Those who are granted access to information and information systems must:

a) Only access systems and information, including reports and paper documents to which they are authorised.
b) Use systems and information only for the purposes for which they have been authorised.
c) Comply with all applicable legislation and regulations.
d) Comply with the controls defined by the Information Owner.
e) Comply with all Harlow Council policies, standards, procedures and guidelines, and the policies and requirements of other organisations when granted access to their information.
f) Not disclose confidential or sensitive information to anyone without the permission of the Information Owner, and ensure that sensitive information is protected from view by unauthorised individuals.

g) Keep their passwords secret, and not allow anyone else to use their account to gain access to any system or information.
h) Notify the IT Service Desk of any actual or suspected breach of information security, or of any perceived weakness in the organisation's security policies, procedures, practices, process or infrastructure in accordance with the Incident Reporting and Management Procedure.
i) Protect information from unauthorised access, disclosure, modification, destruction or interference.
j) Not attempt to disable or bypass any security features which have been implemented.
k) All users are responsible for reporting any actual or suspected information security incidents or problems and assisting with their resolution.
l) The Senior ICT Manager is responsible for managing the resolution of each incident and its underlying problem.

7. Approach to Risk Management

Risk management is defined as co-ordinated activities to direct and control an organisation with regard to risk.

Harlow Council's approach to information security is through the risk management process to focus on providing the business with an understanding of risks to allow effective decision making to control risks. The risk management process is an ongoing activity that aims to continuously improve the efficiency and effectiveness of information security.

8. Incident Reporting and Management

Harlow Council has established an Incident Reporting and Management Policy This Policy is managed by the Senior ICT Manager with direct liaison through the IT Service Desk.

9. Review

The Essex On-Line Partnership will undertake an annual review of information security policies and associated papers to ensure they still comply with current good practice and standards as well as an equality impact assessment if policies change. It is the duty of Harlow Council to review information security management arrangements in place and review local arrangements contained within local policies, including an IT Health Check carried out by an accredited independent expert.

10. Awareness, Compliance and Auditing

Harlow Council will ensure compliance with the Corporate Information Security Policy through:

10.1 Awareness

a. Information security will be included in the induction programme.

b. An ongoing information security awareness programme will be implemented for all users including third parties.

c. All users will receive appropriate awareness training and updates in organisational policies and procedures as relevant to their job functions.

d. All users will be required to sign a personal commitment statement.

10.2 Compliance

Compliance with this Policy is mandatory, and non-compliance with it and supporting policies, procedures and standards may result in disciplinary action, or termination of contracts under which a business provides services.

10.3 Auditing

a. Carrying out internal audits and where appropriate keeping audit logs in line with legislation and Harlow Council Records Management Policy.

b. Where connectivity to other secure networks such as N3 or GSi is established, Harlow Council will submit to (and fund) an audit of their security procedures and practices in the form of an annual IT Healthcheck, and implement any recommendations to demonstrate that they meet the requirements of this Policy.

11. Monitoring

Where appropriate, monitoring arrangements are put in place to ensure compliance with policy objectives, guidelines and standards.

Version History

Date of this revision: 11th September 2014
Date of next planned revision: September 2015

Version No:	Version date	Summary of Changes	Revised by
0.1	October 2007	First draft	EOLP Resource Team
1.0	28th March 2008	Changes agreed by the EOLP Information Security working group on 17-03-08.	EOLP Resource Team
2.0	20th February 2009	Changes agreed by the EOLP Information Security working group on 05-02-2009.	EOLP Resource Team
2.1	30th June 2009	Equality Impact Assessment carried out changes to Section 9 Review to include EQIA and Section 12 Documentation to provide the policy in the required format	EOLP Resource Team
2.2	25th January 2010	Combined all policies into the Corporate IS Policy and created a set of Technical Control in support of this policy.	EOLP Resource Team
2.3	112th February 2010	Moved Definitions to Technical Control spreadsheet, minor changes following Information Security working group meeting.	EOLP Resource Team
3.0	1st March 2010	Removed the highlights that indicated the changes that were made.	EOLP Resource Team
3.1	23rd June 2011	Incorporated PSN CoCo requirements	EOLP Resource Team
4.0	14th July 2011	Incorporated feedback from ISWG	EOLP Resource Team
5.0	27th September 2011	Additional text for Information Owners and added role of Risk Manager, text taken from PSS IA glossary. Changes to Approach to Risk and Incident Management	EOLP Resource Team
5.1	January 2012	Localised changes for Harlow Council	Declan White
0.1	October 2007	First draft	EOLP Resource Team
1.0	28th March 2008	Changes agreed by the EOLP Information Security working group on 17-03-08.	EOLP Resource Team
2.0	20th February 2009	Changes agreed by the EOLP Information Security working group on 05-02-2009.	EOLP Resource Team
2.1	30th June 2009	Equality Impact Assessment carried out changes to Section 9 Review to include EQIA and Section 12 Documentation to provide the policy in the required format	EOLP Resource Team
2.2	25th January 2010	Combined all policies into the Corporate IS Policy and created a set of Technical Control in support of this policy.	EOLP Resource Team
2.3	112th February 2010	Moved Definitions to Technical Control spreadsheet, minor changes following Information Security working group meeting.	EOLP Resource Team
3.0	1st March 2010	Removed the highlights that indicated the changes that were made.	EOLP Resource Team
3.1	23rd June 2011	Incorporated PSN CoCo requirements	EOLP Resource Team
4.0	14th July 2011	Incorporated feedback from ISWG	EOLP Resource Team
5.0	27th September 2011	Additional text for Information Owners and added role of Risk Manager, text taken from PSS IA glossary. Changes to Approach to Risk and Incident Management	EOLP Resource Team
5.1	January 2012	Localised changes for Harlow Council	Declan White
5.2	11th Sept 2014	Latest revision	Declan White

Appendix A

This is a list of key legislation and regulations.

Data Protection Act 1998 and the EU Directive on Data Protection

Personal information relating to identifiable individuals must be kept accurate and up to date. It must be fairly obtained and securely stored. Personal information may only be disclosed to people who are authorised to use it.
Unauthorised disclosure of Harlow Council or client personal information is prohibited and could constitute a breach of this Act.

Freedom of Information (FOI) Act 2000/Environmental Information Regulations 2004

These give a general right of access to all types of data and information that has been recorded by the Council. There are exemptions to the right of access, but the Council must assist applications for information and proactively make details available about the Council. The Council must know what records it holds, where they are stored and must avoid them being lost.

Further information on Data Protection and FOI can be obtained from the Corporate Information Manager, Marie Bentley on tel. 01279 446736 or email marie.bentley@harlow.gov.uk.

Computer Misuse Act 1990

Deliberate unauthorised access to, copying, alteration or interference with computer programs or data is not allowed and constitute an offence under this Act for which the penalties are imprisonment and/or a fine.

This Act addresses the following offences:

a) Unauthorised access to computer material.
b) Unauthorised access with intent to commit or facilitate commission of further offences.
c) Unauthorised modification of computer material.

Further information on these Acts can be obtained from Declan White on tel. 01279 446146 or email declan.white@harlow.gov.uk.

Copyright, Patents and Designs Act 1988

Documentation must be used strictly in accordance with current applicable copyright legislation, and software must be used in accordance with the licence restrictions. Unauthorised copies of documents or software may not be made under any circumstances.

Companies Act 1985

Adequate precautions should be taken against the falsification of records and to discover any falsification that occurs.