Colchester

essexonline

Done Once, Shared By Many

Corporate Information Security Policy

A guide to the Council's approach to safeguarding information resources.

September 2015

Contents

Page

1. Introduction

Information resources are vital to Colchester Borough 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 perception of the Council.

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

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

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

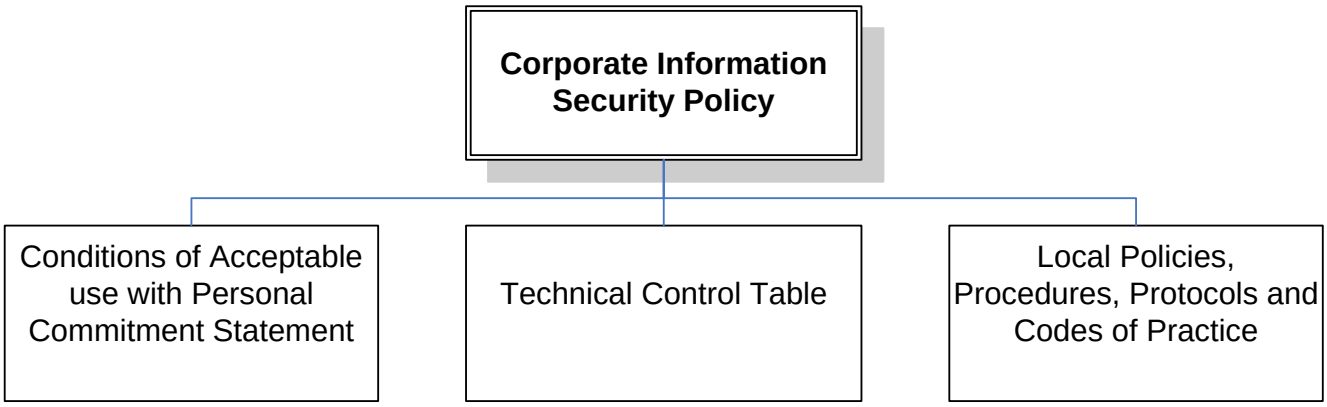
This policy is designed to provide an appropriate level of protection to the information for which the Council is responsible. Supporting this policy is a set of information security technical controls which form the minimum standard that an Essex OnLine partner has to comply with. Individual organisations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

It is unacceptable for Colchester Borough 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 Council 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.

2. Information Security Framework



3. Objectives

The objectives of the Corporate Information Security Policy are to ensure that:

- All users are aware of these policy statements and associated legal and regulatory requirements and of their responsibilities in relation to Information Security.
- All Council property, including equipment and information, is appropriately protected.
- The availability, integrity and confidentiality of Council information are maintained.
- A high level of awareness exists of the need to comply with Information Security measures.
- Unauthorised access to software and information is prevented.
- The risk of the misuse of email services is reduced.
- The network and network resources are protected from unauthorised access.
- Guidance is provided on handling information of each classification in different circumstances and locations including creation, modification or processing, storage, communication, retention and deletion, disposal or destruction.
- Unwanted incidents such as virus infections, deliberate intrusion and attempted information theft are managed.
- Any unauthorised access, damage and interference to business premises, Information and Information Technology is prevented.

4. Audience

The audience for this policy is for any employee, elected member, agency worker, third party organisation or other authorised personnel. Stakeholders are entitled to view the policy.

5. Legal and regulatory obligations

Colchester Borough Council will comply with all relevant legislation affecting the use of information and communication technology. All users must 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

- **Accountable Officer**

The Chief Executive Officer for Colchester Borough Council is ultimately responsible for ensuring that all information is appropriately protected.

- **Information Security Management Group**

This policy has been written by the Essex OnLine Partnership, additional policies, procedures and standards are written by Corporate ICT at Colchester. Corporate ICT are responsible for reviews and approval of Security Policies, which are reviewed and re-issued each year. They are also responsible for approving and overseeing all information security related projects and initiatives. Colchester Borough Council appoints a Senior Information Risk Owner (SIRO) to ensure there is accountability.

The SIRO must provide written judgement of the security and use of the business assets at least annually to support the audit process and provide advice to the Accountable Officer on the content of their statement of internal control.

- **Information Security Management**

This function is fulfilled within the Corporate ICT team who are responsible for the day to day management of information security activities, and for responding to Information Security Incidents. The Head of Security is the ICT Manager.

- **SIRO (Senior Information Risk Owner)**

The SIRO

- Is the officer who is ultimately accountable for the assurance of information security at the Council
- Champions information security at executive management team level
- Owns the corporate information security policy
- Provides an annual statement of the security of information assets (as part of the audit process)
- Receives strategic information risk management training at least once a year

The SIRO is not concerned solely with IT but takes a broader view of our information assets as a whole, in any form.

- **Risk Manager**

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

- **Information Owners (also referred to as Information Asset Owners)**

The role of Information Asset Owners is to understand what information is held and in what form, how it is added and removed, who had access, and why. They are tasked with ensuring the best use is made of information, and receive and respond to requests about it.

They are responsible for:

- Assessing the risks to the information and data for which they are responsible in accordance with the Risk Management Methodology of the Council.
- Defining the appropriate protection of their information taking into consideration the sensitivity and value of the information.
- Defining the value of information, and identifying the risks associated with the information, so they must classify their information, and define the controls for its protection.

- **Directors, Heads of Service and Line Managers**

Managers are responsible for:

- 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.
- Developing procedures, processes and practices which comply with this Policy for use in their business areas.
- Ensuring that all external agents and third parties acting on behalf of their business area are aware of their requirement to comply.
- Ensuring that when requesting or authorising access for their staff, they comply with the standards and procedures defined by the Information Owners.
- Notifying the Head of Security of any suspected or actual breaches or perceived weaknesses of information security.

- **Employees**

Staff are responsible for:

- Ensuring that they conduct their business in accordance with this Policy and all applicable supporting policies.
- Familiarising themselves with this Policy, and all applicable supporting Policies, Procedures, Standards and Guidelines.
- Responsible for reporting any actual or suspected Information Security Incidents or Problems and assisting with their resolution.

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:

- Only access systems and information, including reports and paper documents, to which they are authorised.
- Use systems and information only for the purposes for which they have been authorised.
- Comply with all applicable legislation and regulations.
- Comply with the controls defined by the Information Owner.
- Comply with all Council Policies, Standards, Procedures and Guidelines, and the policies and requirements of other organisations when granted access to their information.
- 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 including other people in the same building or location.
- Ensure that, if working from home, adequate physical and other security measures are in place in their homes to prevent any unauthorised access to CBC equipment or information.
- Keep their passwords secret and not allow anyone else to use their account to gain access to any system or information.
- Notify Corporate ICT 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.
- Protect Information from unauthorised access, disclosure, modification, destruction or interference.
- Not attempt to disable or bypass any security features which have been implemented.
- Be responsible for reporting any actual or suspected Information Security Incidents or Problems and assisting with their resolution. Corporate ICT are responsible for managing the resolution of each incident and its underlying cause.

7. Approach to Risk Management

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

The approach of the Council to information security is in accordance with the PSN Risk Management & Accreditation Reference Document as published by the Cabinet Office.

8. Incident Reporting and Management

The Council has established an Incident Reporting and Management framework which is in accordance with the PSN Incident and Problem Management Document as published by the Cabinet Office. That part of this policy is managed by Corporate ICT.

9. Review

The Essex OnLine Partnership must 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 Colchester Borough 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. Accreditation can be with CHECK, an accreditation framework from CESG the Information Assurance (IA) arm of GCHQ, based in Cheltenham, Gloucestershire.

10. Awareness, Compliance and Auditing

The Council will ensure compliance with the 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.

10.2 Compliance

Compliance with this Policy is mandatory, and non-compliance with this Information Security Policy, 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 Colchester Borough Council document retention policy.
b. Where connectivity to other secure networks such as N3 or GSi is established, the Council must submit to (and fund) an audit of their security procedures and practices in the form of an annual IT Health Check, and implement any recommendations to demonstrate that they meet the requirements of this security policy.

11. Monitoring

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

12. Documentation

Document Owners: Essex OnLine Partnership Management Group and Colchester Borough Council

Document Authors: Essex OnLine Partnership Resource Team and Colchester Borough Council

Disclaimer:

A printed version may not be the current version.

A current version may be obtained in the required format from the EOLP Resource Team or from Colchester Borough Council's Corporate ICT team.

Version History

Version	Release Date	Update Authorised by	Update carried out by	Update Approved by	Changes
0.1	Oct 2007	EOLP	EOLP Resource Team		First draft
1.0	28th Mar 2008	EOLP	EOLP Resource Team	EOLP Information Security Working Group (ISWG)	Changes agreed by the EOLP Information Security working group on 17-03-08.
2.0	20th Feb 2009	EOLP	EOLP Resource Team	EOLP ISWG	Changes agreed by the EOLP Information Security working group on 05-02-2009.
2.1	30th June 2009	EOLP	EOLP Resource Team	EOLP ISWG	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
2.2	25th Jan 2010	EOLP	EOLP Resource Team		Combined all policies into the Corporate IS Policy and created a set of Technical Control in support of this policy.
2.3	112th Feb 2010	EOLP	EOLP Resource Team		Moved Definitions to Technical Control spreadsheet, minor changes following Information Security working group meeting.

Version	Release Date	Update Authorised by	Update carried out by	Update Approved by	Changes
3.0	1st March 2010	EOLP	EOLP Resource Team	EOLPMG	Removed the highlights that indicated the changes that were made.
3.1	23rd June 2011	EOLP	EOLP Resource Team		Incorporated PSN CoCo requirements
4.0	14th July 2011	EOLP	EOLP Resource Team	EOLP ISWG	Incorporated feedback from ISWG
5.0	27th Sept 2011	EOLP	EOLP Resource Team	EOLP ISWG	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
5.1	18th Oct 2012	EOLP	EOLP Resource Team	EOLP ISWG	Risk Manager section changed DSO to SIRO
6.0	Nov 2012	EOLP	EOLP Resource Team	EOLP ISWG	Version 6 Issued
6.1	June 2013	CBC	CBC Information Team		Version 6.1 Issued
6.2	Sept 2014	CBC	Asa Aldis – Information Security Officer		Reference to ISO2700 updated. Reference to Information Team removed
6.3	9 Sep 2015	CBC	ICT Manager	CBC Management	Minor grammatical and formatting changes. Removal of references to the Information Security Officer. Insertion of references to the ICT Manager as Head of Security. Removal of the obligation for ALL users to sign a personal commitment statement.

Appendix A

This is a list of key legislation and regulations.

Data Protection Act 1998 and 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 Council or client personal information is prohibited and could constitute a breach of this Act.

Further information on this Act can be obtained from Corporate ICT: admin.CorporateICT@colchester.gov.uk.

Computer Misuse Act 1990

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

This Act addresses the following offences:

- Unauthorised access to computer material.
- Unauthorised access with intent to commit or facilitate commission of further offences.
- Unauthorised modification of computer material.

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.

Freedom of Information Act 2000

This Act gives 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 this Act can be obtained from Corporate ICT: admin.CorporateICT@colchester.gov.uk.