# Corporate Information Security Policy

**Version Control Sheet**

| | |
|---|---|
| ***Title:*** | Corporate Information Security Policy |
| ***Purpose:*** | To advise staff of the Council's responsibilities for Information Security<br>To advise staff of the procedures to follow in relation to safeguarding information. |
| ***Owner:***<br>***Author:*** | Data Protection Advisor<br>lhenley@Thurrock.gov.uk<br>01375 652500 |
| ***Approved by:*** | |
| ***Date:*** | March 2019 |
| ***Version Number:*** | 1.0 |
| ***Status:*** | Draft |
| ***Review Frequency:*** | As and when changes take place to Information Governance Legislation. |
| ***Next review date:*** | As above |

## CONTENTS

## 1. Introduction

Information resources are vital to Brentwood Borough Council ‘’herein referred to as *the 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 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 made available to Brentwood under secondary disclosure agreements is also treated appropriately by Brentwood.

Any public authority 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.

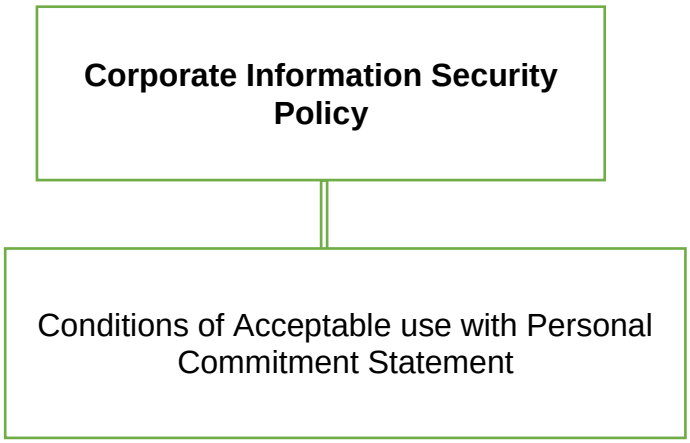
The Chief Executive of Brentwood Borough council has ultimate responsibility and endorses the adoption and implementation of this Information Security policy.

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 a partner has to comply with. Individual organisations can strengthen these policies through local policies and procedures but cannot weaken them.

It is unacceptable for the council’s information resources to be used to perform unethical or unlawful acts.

This Corporate Information Security policy is supported by further policies, procedures, standards and guidelines as detailed in **Appendix B**. In addition to the council’s 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 objective of the Corporate Information Security Policy is 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's properties including equipment and information is appropriately protected.
- The availability, integrity and confidentiality of the council information is maintained.
- A high level of awareness exists of the need to comply with Information Security measures.
- To prevent unauthorised access to software and information.
- To reduce the risk of the misuse of e-mail services.
- To protect the network and network resources from unauthorised access.
- 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.
- To manage unwanted incidents such as virus infections, deliberate intrusion and attempted information theft.
- To prevent unauthorised access, damage and interference to business premises, Information and Information Technology.

## 4. Scope

The scope of this policy is for any employee, elected member, agency worker, third party organisation or other authorised personnel.

## 5. Legal and regulatory obligations

The 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

- **Chief Executive Officer**

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

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

The council has appointed a Senior Information Risk Owner (SIRO) to ensure there is accountability and this officer is Director who has responsibility for Commercial Services. 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 accounting officer on the content of their statement of internal control.

Local Government Association guidance and best practice suggests that 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 intended to be a new post but rather a newly-defined set of responsibilities for an existing 'board-level' post. It is not concerned solely with ICT, 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.

- **Information Governance Group**

Information Champions made up of individuals (who will come together as an Information Governance Group) will be nominated with the responsibility for the implementation and monitoring of information governance across the Authority. The work undertaken by Information Champions will be in line with the Information Governance Group's Terms of Reference.

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

The role of the Information Asset Owner 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 request

They are responsible for:

- Assessing the risks to the information and data for which they are responsible in accordance with the council's Risk Management Methodology.
- Defining the appropriate protection of their information taking into consideration the sensitivity and value of the information.
- Information owners will be responsible for 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**

  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 defined in the scope of this policy 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 Strategic lead - Information Management of any suspected or actual breaches or perceived weaknesses of information security.

- **Employees**

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.

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 Brentwood 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.
- Keep their passwords secret, and not allow anyone else to use their account to gain access to any system or information.
- Notify the Data Protection team 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.

## 7. Approach to Risk Management

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

The 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.

The council **should** complete a Corporate Information Risk Plan, reviewing all assessments and examine forthcoming potential changes in services, technology and threats.

## 8. Incident Reporting and Management

The council has established an Incident Reporting and Management framework which is supported by this policy. That part of this policy is managed by the Data Protection team

## 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 Brentwood Council to review the 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

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.

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 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 Brentwood's document retention policy.
b. Where connectivity to other secure networks such as N3 or GSi is established, Brentwood **must** submit to (and fund) an audit of their security procedures and practices in the form of an annual ICT Healthcheck, 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.

**Appendix A -** This is a list of key legislations and regulations.

### Data Protection Act 2018

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 Regulation. Further information on this Regulation can be obtained from the Data Protection Team.

### 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

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 can be provided through the Data Protection Team.

## Appendix B – Supporting Policies

Below is a list of policies in support of the Information Security Policy:

- Clear Desk Policy
- Data Protection Policy Statement
- Data Breach Policy
- Security Classification and Data Handling Policy
- Conditions of Acceptable Use
- Document Retention Policy
- Freedom of Information Policy
- Data Security and Encryption Policy
- Records Management Policy
- Email Policy
- Information Request Charging Policy