Tendring District Council

Corporate Information Security Policy

October 2018

Version Control Sheet

Title	Corporate Information Security Policy
Author	Sam Wright, Cyber Security & Systems Manager Judy Barker, Information Governance & IT Services Manager
Approved by	IGPU & HR Committee, Approval & Adoption
Date	May 2018
Version Number	1
Status	DRAFT
Review Frequency	Annually or as required to meet changes in legislation
Next Review Date	October 2019

Amendment History / Change Record

Date	Version	Key Changes / Sections Amended	Amended By
16/03/17	0.1	1st draft following amendments to EOLP base policies	Sam Wright
26/09/17	0.2	2nd draft incorporating amendments from feedback and recommendations	Sam Wright / Judy Barker
17/05/18	1	Final review before submission for approval and adoption	Sam Wright / Judy Barker

Contents

1. Introduction

Information is essential to delivering services to our residents, businesses and visitors. Their availability, integrity, security and confidentiality are essential to maintain service levels, legal compliance and the public image/perception of the Council.

It is important that our customers are able to trust Tendring District 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 Tendring District Council is treated appropriately by the Council. The same applies to information we share with others under Information Sharing Protocols (ISP).

This Corporate Information Security Policy is supported by further policies, procedures, standards and guidelines. 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 should be provided before access is granted.

Information security refers to the defence of information and/or information systems from unauthorised or unintended access, destruction, disruption or tampering. It is essential that our organisation acts appropriately with the information we obtain, hold and process. Confidentiality, integrity and availability of information must be proportionate and appropriate to maintain services. We must provide assurance to our customers and partners that we meet all legal obligations under information governance legislation (such as Data Protection Act, General Data Protection Regulations, Freedom of Information & Environmental Information Regulations) and any other legal requirement.

2. Policy Statement and Scope

This policy applies to everyone who accesses any information that the organisation holds and are required to familiarise themselves with the content of these policy statements and their responsibilities in relation to information security.

Tendring District Council commits to informing all employees, members, voluntary workers, agency staff, contractors and other third parties of their obligations before they are authorised to access systems and information and then subsequently at regular intervals thereafter. Other organisations granted access to information held by the Council must abide by this policy.

All individuals who access information have a personal responsibility to ensure that they comply with this policy.

This policy will be reviewed by the Information Governance Policy Unit in accordance with its IT Policy Review Schedule.

3. Obligations

You must;

- Only access systems and information for which you are authorised to use/view, including reports and paper documents.
- Only use systems and information for the purposes for which it was collected.
- Comply with all applicable legislation and regulations.
- Comply with controls communicated by the Information Owner / System Sponsor.
- Comply with all Tendring District 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 (Special Category) information to anyone without a lawful basis to do so and the permission of the Information Owner / System Sponsor.
- Ensure confidential or sensitive (Special Category) information is protected from view by unauthorised individuals.
- Not attempt to disable or bypass any security features which have been implemented.
- Not copy, transmit or store information to unauthorised devices or locations (physical or digital).
- Ensure appropriate levels of security are in place on devices and in locations to provide adequate protection for information. e.g. The more sensitive the data, the higher levels of security required.
- Protect information from unauthorised access, use, disclosure, modification, destruction or interference.
- Keep passwords secret and do not allow anyone else to use your access to systems and accounts.
- Notify the IT Service Desk promptly of any actual or suspected breach, weakness or perceived risk associated with Information Security and buildings (e.g. break in, loss/theft of a device or file).
- Co-operate with compliance, monitoring, investigatory or audit activities.

4. Roles and Responsibilities

The Organisation

- Corporate Compliance with laws governing the processing and use of information.
- Tendring District Council has an Information Security / Information Management Incident Reporting and Response procedure to comply with legislative requirements.

The Chief Executive

- Ultimately responsible for ensuring that all information is appropriately protected.

Senior Information Risk Owner (SIRO)

- Assures information security within the organisation.
- Ensures appropriate internal compliance audits.
- Owns the Corporate Information Security Policy.
- Promotes information security at executive management level.
- Provides an annual statement about the security of information assets.

Information Governance Policy Unit (IGPU) & Information Security Management Team (ISMT)

- IGPU has overall responsibility for the development and/or adoption of new policies, procedures and standards affecting information governance including consideration of risk assessments and risk ratings identified by the Information Security Management Team.
- ISMT has responsibility for implementing directives made by IGPU and overseeing all information security related projects, working closely with internal audit and the Corporate Data Protection Manager.

Cyber Security Manager

- Ensures annual IT Health Checks are conducted by suitably certified parties to meet Public Services Network (PSN) and other security requirements.

- Maintain a current knowledge of security issues, standards, threats and vulnerabilities.
- Manages the remediation and mitigation of identified IT security vulnerabilities.
- Manages the investigation and mitigation of information breaches.
- Promotes the requirement to assess risks, implement controls, including Privacy Impact Assessments (PIA's) and the incorporation of Privacy By Design and Privacy By Default in all new procurement or development initiatives.
- Work closely with the Data Protection Manager on all aspects of Information Security and to support legal compliance.

Data Protection Manager

- Be involved in all aspects relating to the protection of personal data and the Rights of data subjects.
- Maintain a current knowledge of legislative requirements.
- Ensure compliance is managed.
- Provide advice and guidance.
- Liaise and cooperate with the UK Information Commissioners Office (ICO) and be identified as the single point of contact for the Council.
- Manage the creation and ongoing maintenance of the corporate information asset register and Privacy Notice(s) based on information provided by the business.
- Work closely with the Cyber Security Manager on all aspects relating to the security of Personal Information.

Information Owners / System Sponsors

- Assess the risks to the information they are responsible for by conducting and maintaining appropriate Privacy Impact Assessments (PIAs).
- Ensure adequate measures are in place to protect the information they are responsible for, taking consideration of the sensitivity and value of the information.
- Communicate the personal data processing requirements of the business to the Data Protection Manager.
- Communicate the protection controls to authorised users and ensure controls are followed.
- Ensure that authorised users attend suitable training to maintain appropriate levels of knowledge.

Directors, Managers and Line Managers

- Ensure their employees are fully conversant with this policy and all associated standards, procedures, guidelines and relevant legislation; and are aware of the consequences of non-compliance.
- Develop procedures, processes and practices which comply with this policy for use in their business areas.
- Ensure that all external agents and third parties defined in the 'Policy Statement and Scope' section above are aware of the requirement to comply.
- Ensure their employees complete all mandatory training required by the Council.
- Ensure that Information Owners / System Sponsors within their business area maintain adequate levels of knowledge to comply with the requirements of this role.
- Ensure all employees are aware of how to access this policy, associated standards and guidelines; including those employees without access to the Councils network and applications.

Employees

- Take responsibility for familiarising themselves with this policy and understand their personal responsibilities and obligations.
- Undertake their duties in accordance with this policy and all other applicable supporting policies, standards and guidelines. Take responsibility for the management of relevant third parties and ensure they comply with this Policy.
- Ensure any compliance issues and/or training needs are raised with their Manager.

5. Applicable Legislation

- Data Protection
- Computer Misuse
- Copyright, Patents & Designs
- Companies Act
- Freedom of Information (FOI)
- Environmental Information Regulations (EIR)
- Privacy and Electronic Communications Regulations (PECR)
- Police & Criminal Justice Legislation