Corporate Information Security Management Policy

Signed: Claire Hamilton **Chief Executive.**

Number:	**DBC001 IS**	**Title:**	**Corporate Information Security Management Policy**				
Owner:	**Info. Security Manager**	**Rev**	**1.3**	**Date**	**2nd December 2020**	**Classification**	**UNRESTRICTED**

1. Definition of Information Security

1.1. Information security means safeguarding information from unauthorised access or modification to ensure its:

- **Confidentiality** – ensuring that the information is accessible only to those authorised to have access;
- **Integrity** – safeguarding the accuracy and completeness of information by protecting against unauthorised modification;
- **Availability** – ensuring that authorised users have access to information and associated assets when required.

2. Policy Statement

2.1. The purpose of the Corporate Information Security Management Policy is to protect the Council's information assets, manage information risk and reduce it to an acceptable level, while facilitating reasonable use of information in supporting normal business activity and that of our partners

2.2. Information is an important asset, the Council is committed to preserving the confidentiality, integrity, and availability of its information assets:

- For sound decision making;
- To deliver quality services;
- To comply with the law;
- To meet the expectations of our customers;
- To protect our reputation as a professional and trustworthy organisation.

3. Scope

3.1. This policy applies to all councillors, employees, partners, contractors and agents of the Council (i.e. users) who use or have access to Council information, computer equipment or ICT facilities.

3.2. The policy applies throughout the lifecycle of the information from creation, storage, and use to disposal. It applies to all information including:

- Information stored electronically on databases or applications e.g. email, ICT Systems supporting back and front office;
- Information stored on laptops, tablets, mobile phones, printers, or removable media such as hard disks, CD rom, memory sticks, memory cards, tapes and other similar media;
- Information transmitted or stored on networks, network file shares;

- Information sent by fax or other communications method;
- All paper records
- Microfiche, visual and photographic materials including slides and CCTV
- Spoken, including face-to-face, voicemail and recorded conversation.

4. Policy Compliance and Disciplinary Action

4.1. All employees, councillors and anyone who delivers services on the Council's behalf e.g. contractors, partners, agents or other third parties with access to the Council's information assets have a responsibility to promptly report any suspected, potential or observed security breach; further details are provided in the 'Personal Data Breach or Incident Reporting Procedure' (DBC999 IS Proc)

4.2. Security breaches that result from a deliberate act or omission or from an otherwise negligent disregard of any of the Council's security policies and/or procedures, may result in disciplinary action being taken against the employee under their contract of employment or, in the case of a councillor, under the Members' Code of Conduct. In the event that breaches arise from a deliberate or negligent disregard for the Council's polices and/or procedures, by a user who is not a direct employee of the Council, or a councillor, the Council may seek to take such punitive action against that user and/or their employer as the Council deems appropriate.

4.3. The Council may refer the matter of any breach of the Council's security policies and/or procedures to the police for investigation and (if appropriate) the institution of criminal proceedings if in the reasonable opinion of the Council such breach has or is likely to lead to the commissioning of a criminal offence

5. Legal and Regulatory Requirements

5.1. Users of the Council's information assets will abide by UK and European legislation relevant to information security, management and technology including;

- GDPR / UK Data Protection Act 2018
- Freedom of Information Act 2000
- Computer Misuse Act 1990 (Amended by the Police and Justice Act 2006)
- Police and Justice Act 2006
- The Privacy and Electronic Communications Regulations 2003
- The Copyright, Designs and Patents Act 1988
- The Electronic Communications Act 2000
- Human Rights Act 1998

- Regulation of Investigatory Powers Act 2000
- Telecommunications (Lawful Business Practice) Regulations 2000
- Civil Contingencies Act 2004
- Public Service Network (PSN)

The list is not exhaustive and may change over time. Users should seek guidance about the legal constraints of using information in their work and the Council will provide the appropriate guidance and training for staff.

5. Roles and Responsibilities

5.1. The Council's Senior Information Risk Officer (SIRO) has responsibility for managing information risk on behalf of the Chief Executive and Corporate Management Team, setting strategic direction and ensuring policies and processes are in place for the safe management of information. The Solicitor to the Council has been designated as the Council's SIRO

5.2. Corporate Directors have responsibility for understanding and addressing information risk within their directorate, assigning ownership to Information Asset/System Owners (Group Managers) and ensuring that within their directorate appropriate arrangements are in place to manage information risk, and to provide assurance on the security and use of those assets.

5.3. Information Asset/System Owners undertake information risk assessment, implement appropriate controls, recognise actual or potential security incidents and ensure that policies and procedures are followed.

5.4. The Information Security Team Leader is responsible for providing, information security advice, and support to all staff, develops appropriate information security, management and technology policies to protect the Council's information, promotes information security awareness, guidance and alerts, attends the relevant forums and best practice groups on information security matters, provides information security training.

5.5. ICT responsible for being the custodian of electronic information in its remit, implementing and administering the appropriate technical security controls

5.6. ALL USERS – Information Security is everyone's responsibility and all employees, councillors, third parties and partners who have access to the Council's information are required to comply with this policy and supporting policies, standards and procedures.

6. Approach to Risk Management

6.1. Information risk will be managed in accordance with the Council's Risk Management Strategy. The Senior Information Risk Officer (SIRO) will have oversight of information risk and the information risk management processes

6.2. In accordance with the Council's Risk Management Strategy, the Corporate Directors are responsible for ensuring critical information assets and systems are subject to information risk analysis on a regular basis. The risk assessment will ensure that; threats and vulnerabilities are identified, risks are assessed, and appropriate decisions are made regarding risks that are accepted and those risks which are to be mitigated by control measures to reduce the risk to an acceptable level.

7. Other Supporting Information Security, Management and Technology procedures.

7.1. This policy is supported by more detailed policies, standards and procedures; these include but are not limited to the following;

7.1.1. DBC010 - IS Corporate Information Technology Security Policy
7.1.2. DBC700 - IS Remote and Home Working Policy
7.1.3. DBC900 - IS Information Security Incident Policy
7.1.4. DBC999 - IS Procedure - Personal Data Breach or Incident Reporting Procedure
7.1.5. DBC100 IM – GDPR / UK Data Protection Act Policy
7.1.6. DBC200 IM - Freedom of Information Act Policy

8. Review of the Corporate Information Security Management Policy

8.1. The current version of this policy will be held on the Council's Intranet (DENNIS>Document Centre) along with information that supports this policy.

8.2. This policy and all supporting procedures will be reviewed at appropriate intervals but no less frequently than every 12 months.

Document Control

Author:	John Worts - Information Security Team Leader
Owner:	Mark Brookes – Solicitor to the Council
Document Number	1.3

Revision History

Revision Date	Previous Revision Date	Previous Revision Level	Summary of Changes	Changes Marked	Next Review Date
30/3/12	n/a	n/a	Rewrite of existing Policy DBC_00001 to ISO27001 standards, to include references to other IS/ICT Policies		
2/4/12	30/3/12	0.1	Added document control tables and changed policy references in section 9.1		
4/4/12	2/4/12	0.2	Agreed reviews from Assistant Director (Legal, Democratic & Regulatory)	All	April 2013
27/6/12	4/4/12	0.3	Minor Changes following discussion at CMT		July 2013
11/7/12	27/6/12	0.4	CMT Approved FINAL		July 2013
19/04/17	11/07/12	1.0	Reflect Structure Changes and PSN		April 2018
25/05/18	19/04/17	1.1	GDPR UK DPA		May 2019
2/12/20	25/5/18	1.2	Removed reference to obsolete GCSX. Removed reference to obsolete hardware. Updated CEO		Dec 2021

Document Approvals

Version	Approved By	Date
1.1	ISTL	19/04/17
1.2	ISTL / CMT	25/05/18
1.3	Legal Governance	2/12/20