I

Eden District Council

Approved by: Council
Date Approved: 26 November 2020
Review Date: November 2022
Responsible Officer: SIRO

Town Hall, Penrith, Cumbria CA11 7QF
Tel: 01768 817817
Email: info.governance@eden.gov.uk

Information Security Policy

Document Control Sheet

Document Control	
Organisation	Eden District Council
Title	Information Security Policy
Author	Information Governance Manager
Filename	InformationSecurityPolicy_2020_v2.0.doc
Owner	SIRO
Subject	Information Security
Protective marking	UNCLASSIFIED
Review date	November 2022

Document Amendment History			
Revision No	**Revised by**	**Date of change**	**Description of Change**
0.1	Information Governance Manager	15 March 2018	Final draft
0.2	Chief Finance Officer and Monitoring Officer	19 March 2018	Governance check amendments
1.0	Information Governance Manager	22 March 2018	Final version
1.1	Information Governance Manager	08 September 2020	Reviewed and updated. Included virtual meetings
1.2	Information Governance Manager	05 October 2020	Incorporated amendments from IT
2.0	Web Admin	30 November 2020	Final version - formatted and accessible

Approval	Date
Corporate Leadership Team	11 November 2020
Council	26 November 2020

Contents

1. Introduction

The information the Council holds and the Information and Communications Technology (ICT) systems and networks that support it are important business assets. Many potential threats to these exist, such as fraud, vandalism, virus infection, theft, loss, abuse of copyright, misuse of software and accidental damage.

The International Standard: ISO 27001:2013 Code of Practice defines Information Security as the preservation of:

- **Confidentiality:** ensuring information is accessible only to those authorised to have access;
- **Integrity:** safeguarding the accuracy and completeness of information by protecting against unauthorised modification; and
- **Availability:** ensuring information and services are available to authorised users when required.

The Council is committed to preserving the confidentiality, integrity and availability of our information assets:

- For sound decision making;
- To deliver quality services;
- To ensure data quality and accurate, up-to-date information;
- To comply with the law;
- To meet the expectations of our customers;
- To protect our customers, staff, contractors, partners and our reputation as a professional and trustworthy organisation;
- To support flexible, remote and home working;
- To enable virtual meetings;
- To ensure the Council can continue working without interruption; and
- To enable secure and appropriate sharing of information.

2. Scope

This Policy is mandatory and there are no exceptions to it. It applies to all employees of the Council, including temporary and contract staff (including agency staff), Elected Members, contractors, agents and partners, who have authorised access to the Council's IT systems.

This Policy applies throughout the lifecycle of information held by the Council on all types of media, from its receipt or creation, storage and use, to disposal.

3. Policy Statement

The Council understands the importance of information security and privacy. We are increasingly dependent on ICT systems and so the potential impact of any breach is also increasing. We must safeguard our information systems and ensure compliance with this

Policy, to provide protection from the consequences of information loss, damage, misuse or prosecution.

The General Data Protection Regulation (GDPR) places a duty on the Council to demonstrate accountability and to have in place the organisational and technical measures to protect the personal data it holds and processes. We are committed to providing the levels of information security required to protect this data and this Policy helps to set out how we aim to achieve the necessary standards.

We also aim to fulfil the business needs of the Council and to allow people to work in a flexible way, whilst maintaining the security levels required.

4. Legal and Regulatory Requirements

The Council has an obligation to ensure all its information systems and information assets and users of those systems and information assets comply with the following:

- Civil Contingencies Act 2004;
- Computer Misuse Act 1990;
- Copyright, Designs and Patents Act 1988;
- Data Protection Act 2018;
- Electronic Communications Act 2000;
- General Data Protection Regulation (GDPR);
- Payment Card Industry Data Security Standard;
- Privacy and Electronic Communications Regulations 2003 and EPrivacy Regulation 2018;
- Public Services Network Compliance; and
- Telecommunications (Lawful Business Practice) Regulations 2000.

If you are unsure about the relevant legal or regulatory requirements relating to the information you use in your work, please contact the Information Governance Manager for guidance.

5. Controls

The Council has information security measures in place to help mitigate risk, known as controls. These controls are divided into three categories: administrative, technical and physical.

5.1 Administrative Controls

5.1.1 Policies and Authorised User Agreements

This written Information Security Policy document is available to all with authorised access to the Council's IT systems. Authorised users are required to read this document and also the ' ICT Acceptable Use Policy.'

- All authorised users must sign the ICT Authorised User Agreement to indicate their acceptance of these policies, before access to the Council's equipment, networkand systems can be granted.

- A process of regular acknowledgement of the Council's information security policies by all authorised users is in place.

5.1.2 Accountabilities and responsibilities

All authorised users of the Council's ICT equipment, network and systems have responsibilities to protect information assets and comply with information security procedures. However, some staff have special responsibilities for maintaining information security:

- **Corporate Leadership Team** - has overall accountability and responsibility for understanding and addressing information risk, including within their own service areas and for assigning ownership for information assets to Information Asset Owners;
- **Senior Information Risk Officer/Owner** (**SIRO)** - the Council's SIRO has overall responsibility for managing information risk on behalf of the Council. The SIRO leads and co-ordinates the Council's Risk Register and Shared IT Services Risk Register;
- **Data Protection Officer (DPO)** - responsible for informing and advising the Council about its obligations in complying with Data Protection laws, for monitoring compliance, advising on Data Protection Impact Assessments and training. The DPO is the first point of contact for supervisory authorities.
- **Information Asset Owners** - responsible for the information assets within their service areas, implementing appropriate controls, recognising actual or potential security incidents and ensuring that policies and procedures are followed.
- **IT Services** - responsible for the development, management and maintenance of all of the Council's IT and communications infrastructure, equipment, systems, processes and procedures.

5.1.3 ICT assets - classification and control

The Council's ICT infrastructure is such that almost all components are considered to be part of a single network.

- No computer, device or hardware shall be acquired or connected to the network and no software shall be installed onto the Council's network or procured (with a view to being installed), without prior approval from IT Services.

Assets are things of value. The Council has many ICT assets and this Policy aims to protect those related to the Council's network. IT Services are responsible for maintaining a database of all ICT assets. This describes the assets, who they are allocated to and records any authorised uses and security procedures related to them.

ICT assets are allocated to an individual, who has use of and is responsible for them. Staff and Members who use portable corporate devices, such as laptops, ipads, tablets and mobiles, must be particularly vigilant, since these devices are more likely to be lost, damaged, or stolen. ICT assets are regularly audited to ensure that no breaches of the Information Security Policy are taking place.

- Corporate portable devices must not be left unsecured in public places.

- Corporate equipment must not be taken abroad unless permission is approved by the SIRO, in consultation with IT Services.

5.1.4 Information security education and training

The Council will seek to provide authorised users with appropriate training, including information security. It is the responsibility of line managers to ensure that staff undertake the training provided.

All new employees and Members are made aware of this Policy and asked to sign it as part of their induction.

5.1.5 Prevention of misuse of ICT facilities

The Council permits authorised users the use of corporate ICT equipment and systems for managed personal use, but this must be in their own time.

- The Council's ICT equipment and systems must not be used for the conduct of personal purposes during working hours, or under any circumstances for private commercial activity. Failure to comply may result in disciplinary action.

5.1.6 Contracts with data processors

Whenever the Council enters into an arrangement with a data processor who will have responsibility for holding and/or processing the Council's data, including personal data, a formal contract containing appropriate safeguards shall be drawn up between that data processor and the Council.

5.1.7 Reporting security incidents

- All security incidents and breaches must be reported immediately, using the procedures set out in the Council's Security Incident Policy or Personal Data Breach Policy, as appropriate. All authorised users have a responsibility to promptly report any suspected or observed incident or data breach.

- Incidents or breaches that result from deliberate or negligent disregard of any security policy requirements may result in disciplinary action being taken.

All incidents will be logged into the IT Service Desk system and reviewed , so that they can be effectively managed and lessons learned.

5.1.8 IT Disaster Recovery Plan and business continuity

It is the responsibility of IT Services to prepare and test an IT Disaster Recovery Plan. The Plan identifies the risks to information and services and steps for reducing those risks and mitigating the potential impact of various types of disaster on business activities.

IT Services are responsible for ensuring that clear and documented procedures exist for operational computer systems considered important to the network. This will allow smooth running in the absence of staff normally responsible for those procedures.

It is the responsibility of IT Services to prepare a Backup Strategy to ensure that important files and information can be copied and protected from damage or loss. The Backup Strategy states that all work should be backed up within 24 hours, without any effort on the part of users.

5.1.9 Control of proprietary software copying

Authorised users must not:

- copy licensed software, install or use unlicensed software. Software is protected by copyright.
- download material such as fonts, drivers, shareware, or freeware, without proper authorisation from IT Services.
- copy or download material or publish it on the Council website, unless they have permission to do so. Much of the material on the internet is protected by copyright.

The Council retains copyright and intellectual property rights over material produced in the normal course of an authorised user's employment, engagement, or association.

5.1.10 Data protection

Personal information on living individuals (who may be identified from the information held) is subject to the Data Protection Act 2018 and GDPR. Compliance with Data Protection legislation is the responsibility of the Council's Data Protection Officer. Authorised users must be aware of their responsibilities for personal data and training is available. Further guidance can be obtained from the Data Protection Officer or Information Governance Manager.

- In the event of needing to share personal data with a contractor or other third party, appropriate safeguards must be written into the contract. If there is no formal contract in place, a Data Sharing Agreement must be completed and signed by all relevant parties. A Data Sharing Agreement template is available on the Corporate Centre.

5.1.11 Safeguarding of organisational records

Important records of the organisation should be protected from loss, destruction and falsification. A corporate Information Asset Register (inventory of key sources of information) is maintained.

5.1.12 Payment Card Industry Data Security Standard

The Payment Card Industry Data Security Standard (PCI-DSS) is a scheme operated by the PCI Security Standards Council on behalf of the payment card companies. The scheme ensures that merchants (including the Council) securely protect card holder data when taking card payments. This includes the environment in which card holder data is collected and processed.

Compliance with PCI-DSS is a mandatory requirement of the Merchant Agreement the Council has with its bank. Failure to comply could be considered a breach of the agreement.

The majority of card holder data is encrypted at the point it is received by the Council's income collection software, which has been certified to comply with the Payment Application Data Security Standards (PA-DSS).

- Where Chip & PIN machines are available these must be used for all 'customer present' transactions. Staff taking card payments over the telephone (or by other verbal means, for example, if there is no access to a Chip & PIN machine) must ensure card details are input directly into the income system and not written down or otherwise record any card numbers, (CVC) security codes or expiry dates.
- Whilst it is not expected customers would submit any card payment details in writing, if this does happen, the details should be securely shredded as soon as the payment has been taken and a note made on the receipting screen that payment details were received in this way.
- Any staff who take card payments, or who may otherwise have access to card holder data in any form, must sign a declaration to this effect and agree to abide by the Council's PCI-DSS Policy.

5.1.13 Virtual meetings

The Council uses Microsoft Team's conferencing technology for the holding of its virtual meetings, including committee meetings. All authorised users are required to follow the guidance below when taking part in virtual meetings:

- When hosting an online virtual meeting, only do so with the Council's corporate account. Personal accounts are not appropriate for this purpose.
- If unsure, check with the host that a meeting is being hosted by a corporate/paid-for account. Free versions of software are often less secure than corporate/paid-for versions and carry increased security risks as a result.
- Do not say anything you would not want to be recorded.
- Do not assume everything shared in a virtual meeting is coming from a valid source.
- Do not assume that everyone at a virtual meeting is there is for a valid purpose.
- As with email, do not open files from untrusted sources.
- Check that the meeting links you receive are from people you trust.
- Remember to check that no sensitive information could be visible, before sharing screens.
- Take care not to share sensitive documents with meeting attendees from outside the organisation who should not have access to them.

5.2 Technical Controls

5.2.1 Access controls and passwords

System access control is achieved through applying access rights and the use of unique user names and passwords. IT Services are responsible for allocating access rights and new passwords and for maintaining appropriate procedures and records.

Privileged accounts are allocated by IT Services on a restricted basis and a record of privileged access is maintained. Privileged access rights for IT staff at network level are only granted for administrative accounts (not personal user accounts). This minimises the risk of an individual member of IT staff inadvertently clicking on a malicious link or installing malware.

Security of passwords is essential. Each authorised user is responsible for the security of their passwords:

- Do not let anyone else know your passwords. Change passwords regularly and choose a password that is hard for others to guess.
- Do not leave a computer that is logged into the network unattended without first locking your screen.

5.2.2 Encryption

All of the Council's laptops and portable corporate devices are securely encrypted and configured using an approved method. Encryption is centrally managed and enforced by IT Services and end users are not able to disable it.

5.2.3 Patches and updates

The Council's computers are properly patched with the latest appropriate updates, to reduce system vulnerability and enhance and repair application functionality. IT Services operate a regular patch process for all servers, computers and devices, which is aligned to relevant patch and update release cycles.

5.2.4 Privacy by Design and DPIA

Privacy by Design is an approach to projects that promotes privacy and Data Protection compliance from the start. Wherever the Council is involved in procuring, developing, or modifying ICT systems or software which involve the holding and processing of personal data, a Privacy by Design approach will be adopted and a Data Protection Impact Assessment (DPIA) will be undertaken.

5.2.5 Security penetration testing

An annual IT health check is performed by a 'Crest' or 'Check' approved organisation and individuals. This health check comprises penetration tests to search for vulnerabilities within the IT infrastructure and is performed both within the corporate network and from outside. This simulates the processes an IT hacker would deploy to try and break into the Council's secure environment.

Any issues arising from the health check are documented in a formal report and remediation plan, whereby they are resolved. Each issue is given a risk score and the issues with the highest risk are resolved first.

This process is a specific requirement of the Council's annual PSN (Public Sector Network) compliance review. The PSN is required to connect the Council to Government departments, such as the DWP, which is needed by Revenues and Benefits for secure data exchange.

5.2.6 Virus controls

IT Services are responsible for developing and monitoring anti-virus measures to protect the Council from computer virus infections and other harmful programs.

Network - the Council's network will detect viruses, whatever their source. If a virus is found on a computer or device, a warning message will appear.

- If you suspect the equipment you are using may be infected, switch off and disconnect from the network. When this is done, report to IT Services immediately.

Personal devices - may not be as well protected as corporate devices and, if infected with a virus, could infect a corporate device.

- Never connect non-corporate devices (any form of removable media) to a corporate device, or to the corporate network.

Portable memory devices - IT Services will issue encrypted USB sticks as required.

Email - email itself is rarely harmful; it is primarily documents, links in emails and programme attached to emails that can contain viruses.

- If you don't recognise the sender, or have any doubts at all about an email, do not open it; it is better to delete it.
- Never open attachments or click on links within an email unless you are certain you know where the email has come from.

Websites - are another source of viruses. The Council's anti-virus software should automatically detect any viruses before anything is downloaded.

- If you see a warning message, leave the website and contact IT Services.
- Be vigilant when browsing the internet and accessing web-based personal email systems using corporate equipment.

If a computer virus is transmitted to another organisation, the Council could be held liable if there has been negligence in allowing it to be transmitted. So always take care, do not open anything suspicious and, if in any doubt, contact IT Services.

5.2.7 Transferring data

Where restricted, confidential, or sensitive data needs to be sent outside of the Council, a secure method must be agreed and documented, in consultation with IT Services.

- Under no circumstances must any restricted, confidential, or sensitive data be copied to any form of removable media.
- Do not use non-corporate devices, such as personal USB memory sticks, to transfer information from, or to corporate devices, or the corporate network.

5.3 Physical Controls

5.3.1 Environmental and backup controls

IT Services and Property Services are responsible for ensuring the adequacy and smooth operation of environmental and backup controls, including:

- Uninterruptible Power Supplies to all critical servers;
- Standby power through a generator; and

- Air conditioning - including temperature and humidity monitoring - both primary and backup.

5.3.2 Server room security

It is the responsibility of IT Services and Property Services to ensure that appropriate security controls are in place for the server room. The server room has additional physical security and is a restricted area.

5.3.3 Disposal of redundant ICT assets

All equipment eventually becomes unusable, or no longer fit for purpose. The Council has procedures in place to deal with the disposal of ICT equipment. It is vital to ensure that all data is destroyed to the appropriate level before any equipment is disposed of. Where an approved recycling organisation is used to dispose of the equipment, they must provide a certificate of destruction.

- All redundant Council ICT equipment must be handed back to IT Services so that it can be disposed of correctly.

6. Compliance with the Information Security Policy

The implementation of this Policy will be monitored to ensure compliance. An audit of software and hardware will be conducted on a regular basis.

- Any breach of this Policy by staff may lead to disciplinary action.
- Any breach of this Policy by a Member may lead to it being referred to the Accounts and Governance Committee.

7. Review

This Information Security Policy will be reviewed by the Information Governance Manager, the Shared IT Services Manager and the SIRO and updated by November 2022.

Accessibility Information

A summary of the information contained in this document is available in different languages or formats upon request. Contact Eden District Council's Communication Officer, telephone: 01768 817817, or email: communication@eden.gov.uk