Report No: G43/20

Eden District Council

Council

26 November 2020

Information Security Policies

Portfolio:	Resources
Report from:	Assistant Director Governance
Wards:	All Wards
OPEN PUBLIC ITEM	

1 Purpose

1.1 To enable consideration to be given to the approval and adoption of revised information security policies and related user agreements.

2 Recommendation

It is recommended that;

(i) The Information Security Policy at Appendix A, the ITC Acceptable User Policy at Appendix B and ITC Authorised User Agreements at Appendix C and D are approved and formally adopted; and

(ii) A process of biennial acknowledgement and signing of the documents by all authorised users is approved.

3 Report Details

3.1 Information security is becoming increasingly important, due to rises in the incidents of cyber-attacks nationally and worldwide and with remote and home working becoming more and more common. Much of the Council's important business and personal data is stored in electronic formats. Given the risks involved, the Council has a responsibility to be vigilant and proactive in protecting the information it holds.

3.2 The Council's current Information Security Policy and Internet and Email Acceptable Use Policy were adopted at a meeting of Executive on 3 April 2018. There have been a number of changes since that time and the policies and user agreements have been revised and updated in line with these changes.

3.3 The updated documents are included as appendices to this report. The policies (which are public documents) will be properly formatted before publishing on the Council's website.

3.4 The appropriate user agreement must be signed in order that an authorised user can be permitted access to the Council's computer network.

3.5 The main changes to the documents are the inclusion of virtual meetings and to reflect increased home and remote working, accelerated by the Coronavirus pandemic.

4 Policy Framework

4.1 The Council has four corporate priorities which are:

- Sustainable;
- Healthy, safe and secure;
- Connected; and
- Creative

4.2 This report meets the ‘sustainable’ corporate priority.

5 Consultation

5.1 A consultation of the policies and user agreements was undertaken with staff, Members and Unison during October 2020. Responses have been received, considered and amendments made where considered appropriate.

6 Implications

6.1 Financial and Resources

6.1.1 Any decision to reduce or increase resources or alternatively increase income must be made within the context of the Council’s stated priorities, as set out in its Council Plan 2019-2023 as agreed at Council on 7 November 2019.

6.1.2 There are no proposals in this report that would reduce or increase resources.

6.2 Legal

6.2.1 The policies seek to ensure compliance with all relevant legislative and regulatory requirements.

6.2.2 A key principle of the General Data Protection Regulation (GDPR) is that personal data is processed securely by means of ‘appropriate technical and organisational measures,’ known as the ‘security principle’.

6.3 Human Resources

6.3.1 There are human resource implications in the signing, returning and checking of user acceptance forms.

6.4 Statutory Considerations

Consideration:	**Details of any implications and proposed measures to address:**
Equality and Diversity	There are no equality and diversity implications.
Health, Social Environmental and Economic Impact	The loss of personal and/or sensitive personal data has health, social and economic implications, particularly for any individuals affected.
Crime and Disorder	The Council has a duty to protect privacy and the personal and confidential data it holds and has in place appropriate policies, procedures and systems to maintain information security.

Consideration:	Details of any implications and proposed measures to address:
Children and Safeguarding	The Council has a duty to protect privacy and the personal data it holds, including in relation to children and vulnerable adults.

6.5 Risk Management

Risk	Consequence	Controls Required
Breach of the Council's information systems and information assets.	Public, financial or reputational harm, to the Council and potentially other organisations and individuals.	Adherence to policies and user agreements.

7 Other Options Considered

7.1 Council could decline to approve the revised documents or alternatively could approve them with amendments.

8 Reasons for the Decision/Recommendation

8.1 To seek to protect the Council's valuable information systems and information assets and the personal and confidential data it holds and processes.

Background Papers:

Appendices:

Appendix A: Information Security Policy

Appendix B: ITC Acceptable Use Policy

Appendix C: ITC Authorised User Agreement - Staff

Appendix D: ITC Authorised User Agreement - Members

Contact Officer: Information Governance Manager

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	DRAFT_InformationSecurityPolicy2020_v1.2.doc
Owner	Assistant Director Finance (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

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

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

ICT
Acceptable Use Policy

Document Control Sheet

Document Control	
Organisation	Eden District Council
Title	ICT Acceptable Use Policy
Author	Information Governance Manager
Filename	ICTAcceptableUsePolicyv1.3.doc
Owner	Assistant Director Finance (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. Added virtual meetings
1.2	Information Governance Manager	05 October 2020	Incorporated amendments from IT
1.3	Information Governance Manager	05 November 2020	Amendment to 7.3 on protected characteristics

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.

ICT is integral to the workplace but its use brings additional responsibilities. This policy explains what these responsibilities are and sets out relevant good practice.

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 access to the Council's ICT equipment, systems and/or who use the Council's network, internet and email facilities.

3. Principles

Access to the Council's network is subject to acceptance of the ICT Acceptable Use Policy and Information Security Policy. You will be given access to the network, internet and email facilities once you have signed the ICT Authorised User Agreement and confirmed that you agree to its terms. .

4. Equipment

ICT equipment will remain the property of Eden District Council and the Council will be responsible for its maintenance for the duration of an authorised user's association with the Council.

Any faults with equipment or issues regarding access to the network should be reported by the authorised user to the IT Service Desk at the earliest opportunity.

Authorised users are to take all steps to protect corporate ICT equipment allocated to them and will be vigilant when using portable devices in unsecured public places. All equipment is to be securely transported and stored.

Any redundant ICT equipment is to be returned to IT Services at the point it is no longer of use. On termination of an authorised user's association with the Council, corporate equipment is to be returned to IT Services.

5. Network

The Council's ICT infrastructure is such that almost all components are considered to be part of a single network. No device or hardware should be acquired or connected to the network and no software shall be installed onto the Council's network or procured , without prior approval from IT Services.

6. Internet

The Council encourages the use of the internet as an efficient form of communication and research.

6.1 Staff are permitted to make personal use of the internet at the discretion of their line manager and in their own time. The Council will not be liable for any loss of personal data or information as a consequence of such use. Acceptable personal use includes:

- Ordering goods online (using personal email addresses);
- Personal banking;
- Personal email accounts (not to be used for official Council business, except for in an emergency situation);
- Accessing websites for things like sports, TV, holiday, travel, insurance, weather; and
- Social networking.

6.2 For security, passwords for such sites should not be saved on a corporate computer or device.

6.3 Staff, contractors, agents and partners may not use the Council's network, internet or email for political activity, involving the expression of support for any particular party, candidate or policy in a General, Local or European election or in any referendum.

6.4 Staff should not post anything relating to Council work related issues on social media or other public sites, without prior approval from their line manager. No material should be posted on public sites which would reflect badly on the Council's reputation or its relationship with clients, business partners or the general public.

6.5 Misuse of internet facilities by staff will be dealt with under the appropriate Disciplinary Procedure. Misuse by Members will involve reference to Accounts and Governance Committee. Misuse by contractors, agents or partners may result in the termination of contract. Misuse includes, but is not limited to the following:

- Visiting, viewing, transmitting or downloading any material from any website containing sexual or illegal material, or which could reasonably be considered as offensive. The Council's firewall will prevent access to most inappropriate sites. However, if you accidentally access such a site, inform IT Services immediately. Failure to do so may be classed as a disciplinary offence. The publication of obscene material is a criminal offence and the definition of 'publication' includes electronic storage or transmission. If anyone is aware of somebody who is visiting harmful or offensive sites, they should report that use to their line manager in the case of staff, to the Monitoring Officer in the case of Members;
- Bullying or harassment;
- Personal use of internet facilities by staff during work time;
- Conducting any private commercial activity, other than ordering personal goods and dealing with personal finances;
- Downloading any copyrighted materials without the permission of the copyright holder;
- Downloading or installing any software without the prior approval of IT Services. IT staff may download and install software as long as it is work-related;

- Wasting the Council's resources, for example by downloading audio, video, photographs, or other large files for personal use;
- Using the internet for gambling, online gaming, accessing chat rooms, or dating;
- Modifying any Council computer, device or web browser software to enable the user to dial directly into any ISP and bypass the security precautions in place;
- Originating or distributing chain letters, junk email or similar correspondence;
- Jeopardising the security of the network by disclosing or sharing passwords and/or impersonating others;
- Gaining or attempting to gain unauthorised access to any computer system of the Council or any other organisation or hack into another website;
- Any breach of relevant legislation such as the Computer Misuse Act; and
- Accessing peer to peer sharing sites.

The Council maintains the right to prohibit access to any particular site as it feels fit, to protect the interests of the Authority.

7. Email

7.1 Personal use

Staff are permitted to access personal email accounts using the Council's ICT equipment and systems, but only in their own time.

Only personal email accounts are tobe used for personal emails. This maintains a distinction between personal activities and work activities. It is particularly the case in relation to personal communications which may become contentious, eg complaints to retailers or other public authorities.

7.2 The legal status

The legal status of an email is similar to any other form of written communication. This means that anything you send using the Council's systems can be considered to be an official communication from the Council.

7.3 Controls

Given the availability for personal use and in order to ensure that the Council is protected from the misuse of email, the following controls will be exercised:

- You must comply with the instructions in this policy;
- Do not think of email as any less formal than a memo or letter. When sending external email take care not to include material which would reflect poorly on the Council's reputation or its relationship with clients, business partners or the general public;
- Never send or store images or text (either internally or externally), which is defamatory, obscene, offensive, abusive, threatening, risqué, in poor taste, or which could reasonably be anticipated to be considered inappropriate;

- Never send or store slurs or jokes around protected characteristics (for example race, sexual preference or gender) ;
- If you are unsure about the appropriateness of any material, then the chances are high that you should not send it;
- Avoid using global lists of email addresses; these should be reserved for exceptional situations. Everyone has more email to deal with than they would like, so it helps to target only the people who really need to receive an email;
- Email takes up space on the servers, which costs money, so delete any emails you do not need to keep. It is a good idea to file any important attachments in a filing system, rather than leaving them in Outlook or MailMeter. Attachments consume by far the largest amount of space. Retention periods for email were introduced in MailMeter in 2018-2019, with auto-delete functions for any emails older than three years. However, this does not apply to mailboxes in Exchange and emails in Outlook may be older than three years.
- If you receive an email that could be considered offensive, bring it to the attention of your line manager.
- Treat colleagues with dignity and respect; and
- Do not use email for gossip.

7.4 Email security

7.4.1 Email is not always secure. If you need to send confidential material, contact IT Services who can advise on setting up secure email.

7.4.2 Take care when clicking on links or opening attachments in emails. It is safest to do this only when you know who sent the link or attachment. Links may lead to phishing sites and attachments may contain malware.

7.4.3 When away from your computer for half a day or more (for whatever reason), set up an ‘out of office’ rule so that people know not to expect a reply. Avoid mentioning that you are on holiday or away from home, as this could have implications for your personal security.

7.4.4 Deletion of email from an account does not result in permanent deletion from the Council's IT systems.

7.4.5 Emails and attachments may need to be disclosed under the Freedom of Information Act 2000, Environmental Information Regulations 2004 and the Data Protection Act 2018. Further information regarding disclosure can be obtained from the Information Governance Manager.

7.4.6 Do not supply the Council's banking details to any person or organisation without prior authorisation from Finance.

7.4.7 Provided that an external party reasonably believes that someone has the authority to negotiate, or enter into an agreement, then the Council will be bound by what that person has said. Email sent by authorised users will usually be acknowledged as originating from the Council, so recipients will in most cases be acting reasonably if they assume that the emails are sent with the Council's authority. Consequently authorised users must exercise particular care in this area of work.

7.4.8 Where organisations accept orders for goods and services via the internet or by email, the facility may only be used provided it complies fully with the Council's Accounting and Audit Rules and all existing creditor payment authorisation procedures.

8. Monitoring

Whilst respecting the privacy of authorised users, the Council maintains the right to monitor and audit the use of email and internet facilities by authorised users to ensure adherence to this Policy. In particular the Council may log the URL (address) of each website visited and the date, time and duration of each visit. The Council may also monitor the email addresses to which emails are sent (or from which they are received) and again, the dates and times emails were sent or opened. Where it is considered that there are reasonable grounds to do so, the Council may open and read an authorised user's' emails.

9. Review

This policy will be reviewed in November 2022, in line with any changes to legal and regulatory requirements, relevant guidance and best practice. by the Information Governance Manager, IT Services Manager and Assistant Director Finance (SIRO).

Eden District Council

ICT Authorised User Agreement – Members

1. I have read and understand Eden District Council's Information Security Policy and ICT Acceptable Use Policy and agree to abide by all the terms set out in them for the duration of my term of office as a Councillor or association with the Council.

2. I will take all steps to protect any Council ICT equipment allocated to me and will be vigilant when using corporate portable devices in unsecured public places. I will return any redundant equipment to IT Services at the point it is no longer of use and all corporate equipment on the termination of my association with the Council.

3. I understand that I may not acquire hardware and connect it to the Council's network or install software on the network or procure it, without prior approval from IT Services.

4. I understand that if I am hosting an online virtual meeting, I may only do so with my corporate Council account, using Microsoft Teams.

5. I am aware that the Council may monitor or examine all or any email or internet traffic and documents initiated, manipulated, responded to or examined by me, where it considers it to have reasonable grounds to do so and without notice to me.

6. I am aware that my email communication may be disclosed in response to a request made to the Council under Freedom of Information Act 2000, Environmental Information Regulations 2004 and the GDPR/Data Protection Act 2018.

7. I am aware that violations of the policies referred to in this agreement may subject me to reference to the Accounts and Governance Committee.

8. I understand that I may be personally liable for any criminal offence, which I may commit in relation to these policies and the use of the Council's network, internet and email facilities.

9. I further understand that my internet and email communications must at all times reflect the good name and character of Eden District Council and protect the image and reputation of the Council.

10. I understand that the policies referred to in this agreement may be amended from time to time and that I will be informed of changes. I accept that I am responsible for ensuring my personal knowledge and understanding of any change to the policies

Member signature: Date:

Printed name:

Eden District Council

ICT Authorised User Agreement – Staff

1. I have read and understand theCouncil's Information Security Policy and ICT Acceptable Use Policy and agree to abide by all the terms set out in them for the duration of my employment or association with the Council.

2. I will take all steps to protect any Council ICT equipment allocated to me and will be vigilant when using corporate portable devices in unsecured public places. I will return any redundant equipment to IT Services at the point it is no longer of use and all corporate equipment on the termination of my association with the Council.

3. I understand that I may not acquire hardware and connect it to the Council's network or install software on the network or procure it, without prior approval from IT Services.

4. I understand that if I am hosting an online virtual meeting, I may only do so with my corporate Council account using Microsoft Teams.I understand that the Council's network, internet and email systems and equipment are to be used for conducting Council business or for personal use (in my own time) only and must not under any circumstances be used for the conduct of private commercial activity.

5. I am aware that the Council may monitor or examine all or any email or internet traffic and documents initiated, manipulated, responded to or examined by me, where it considers it to have reasonable grounds to do so and without notice to me.

6. I am aware that my email communication may be disclosed in response to a request made to the Council under Freedom of Information Act 2000, Environmental Information Regulations 2004 and the GDPR/Data Protection Act 2018.

7. I am aware that violations of the policies referred to in this agreement may subject me to disciplinary action, up to and including dismissal from employment or termination of contract (in the case of a contractor or partner).

8. I understand that I may be personally liable for any criminal offence which I may commit in relation to the policies and the use of the Council's network, internet and email facilities.

9. I further understand that my internet and email communications must at all times reflect the good name and character of Eden District Council and protect the image and reputation of the Council.

10. I understand that the policies referred to in this agreement may be amended from time to time and that I will be informed of changes. I accept that I am responsible for ensuring my personal knowledge and understanding of any change to the policies.

Signature: Date:

Printed name: Post: