East Lothian Council

Policy for the Acceptable Use of ELC Information Systems and IT Infrastructure

Contents

1. Change History

Version	Date	Reviewed By	Approved By	Summary of Change
6	05/2022	S Buczyn		Redraft/major update
6.1	06/2022	C Turnbull		Rewording and review
6.11	11/2022	C Turnbull		Formatting and final review pre-launch

Note: The policy shall be periodically revised and amended in order to ensure that, in the light of any applicable legislative changes, organisational policies or new/increased risks it continues to be effective. All ELC employees will be informed of the updates to this policy. A reference copy of this policy can be found on the ELC intranet, and can also be provided by your line manager.

2. Introduction

This policy forms part of our Council's alignment with ISO27002:2005 'Code of Practice for Information Security Management' and is intended to increase the integrity, confidentiality, availability and protection of East Lothian Council's (ELC) data, information systems and wider IT infrastructure. The scope covers on premise activity, internet-based 'cloud' activity and staff activity while working outside of ELC premises.

Information security is not just about the IT hardware or the electronic files that sit on a computer or on central servers, it covers every piece of knowledge that we possess and store, including manual records and intellectual property.

East Lothian Council treats all aspects of information security with the utmost seriousness. All users who have access to ELC data and/or IT facilities must comply with this 'Acceptable Use Policy' (AUP) as well as the ELC Information Security Policy. Failure to comply may lead to disciplinary procedures being invoked and in certain circumstances actions being reported to the police or legal action taken.

The Chief Executive and the Council Management Team (CMT) fully support this policy and will ensure that it is complied with.

3. Legislation and Code of Practice

The purpose of the Policy is to protect the IT Infrastructure & data/information assets owned and used by East Lothian Council from threats, whether internal or external, deliberate or accidental and to meet all regulatory and legislative requirements, which include but are not limited to:

- Data Protection Act (2018)
- UK General Data Protection Regulation (GDPR) (2021)
- Computer Misuse Act (1990)
- Communications Act (2003)
- Copyright, Design and Patents (1988)
- Obscene Publications Act (1959)
- The Intellectual property Act (2014)
- Freedom of Information (Scotland) Act (2002)
- Human Rights Act (1998)

Codes of practice and legislations listed for IT facilities must be complied with by you as a user of ELC IT infrastructure and data.

This policy forms part of your contractual obligations while working for or on behalf of ELC. Access to certain information systems may also require your signature and agreement of a local system access policy.

The Council will supply guidance on this policy. When users access any Council system through their unique logon this constitutes agreement with the terms of this policy.

4. Purpose

The aim of this policy is to specify end user responsibilities regarding the responsible, professional, legal and ethical use of ELC Information Technology (IT) infrastructure and associated data.

4.1 Data (information) and our IT infrastructure are important assets of East Lothian Council, and all users have a responsibility for protecting those assets from unauthorised access, modification, destruction or disclosure. Information referred to in this policy as confidential is defined as sensitive or personally identifiable information. Information about Council systems or how to access these systems is also deemed as confidential. Information Security is the method of ensuring:

- Confidentiality – Information is not made available or disclosed to unauthorised individuals, entities or processes.
- Integrity – Accuracy and completeness of information.
- Availability – Information is accessible and usable upon demand by authorised users.

4.2 ELC recognises the benefits of the effective and appropriate use of information and communication technology and wishes to encourage the best use of this important facility.

4.3 The Council has a responsibility to ensure that IT systems and equipment are used effectively and efficiently for the needs of the service and are not misused. The Council also has a duty to protect the security and integrity of its systems, equipment and data.

4.4 This policy's aim is not to impose unnecessary restrictions but rather to ensure that all users are fully aware of the rules and to enable them to make appropriate use of Council systems and information assets (see description of scope in section 5.2).

4.5 The Council further recognises the important role of information and communication technology (ICT) in teaching and learning in the authority's schools. This policy seeks to ensure that the availability of these facilities is maximised through the provision of appropriate guidance and controls for teaching staff.

4.6 This version of the policy supersedes all previous ones. Each user is required to comply with this policy. Confirmation of acceptance of the policy is also by using the IT facilities referred to within. By using any of these IT facilities or accessing any data, you are confirming that you have read, understood, and agree to abide by this policy. Failure to comply with the policy will result in your access to ELC systems being terminated.

5. Definitions

5.1 All references in this document to the "Council" or "ELC" shall be deemed to refer to East Lothian Council.

5.2 The 'systems' of the Council are defined as any and all means used by the Council and its users to communicate or store data, both within and outside the Council. These systems include but are not limited to:-

- Data/information – citizen, business and any other data required by ELC to provide services;
- Voice (fixed line, mobile or online platforms such as Skype for Business and Microsoft Teams) and associated software such as mobile apps;
- Portable equipment, including laptops, USB storage devices, tablet computers;
- PCs and associated software;
- Voice and communications network and associated infrastructure;
- Electronic data/information platforms, internal mail, voicemail, servers, applications, mobile devices (such as tablets and smartphones), internet access, fax, photocopiers, printers, multifunction devices and any software, wiring, cloud systems or other network capabilities used to access those forms of communication;
- Physical access to buildings and housekeeping procedures;
- Remote/mobile working platforms, hardware and software.

5.3 The 'users' of the Council 'systems' relates to but is not restricted to the following people – permanent staff, Councillors, contractors, temporary staff, agency staff, secondments, 3rd parties, partner organisations, student internships and any other staff or volunteers as agreed by the IT Service.

6. Scope

This policy forms part of the Council's Information Security Management System (ISMS).

6.1 All ELC employees and any other individuals as described in 5.3 are required to comply with this policy, in order for our information security systems to be secure and effective.

6.2 The policy includes all uses of information and IT infrastructure on the Council premises, even when the Council does not own the equipment, all information technology provided by the Council wherever it is used, and to all external access to the ELC IT facilities from wherever this is initiated.

6.3 The policy is Council policy and is not a collective agreement. It has previously been subject to consultation with the Joint Trade Unions.

6.4 All heads of service, managers and supervisors must ensure that all members of their teams who are likely to make use of ELC systems are aware of their obligations under this policy.

6.5 Any individuals not in paid employment of East Lothian Council, but making use of the systems and information assets must be made aware by the management team in the relevant ELC service area of their obligations under this policy.

6.6 The scope covers all access to ELC systems both in ELC buildings and remotely.

7. Roles and Responsibilities

7.1 This policy has been issued with the authority of the Chief Executive and the Council Management Team and compliance with its principles is mandatory for all users accessing any systems or information assets owned or operated by the Council.
7.2 This policy is managed and controlled by the Head of Corporate Support. The Council's IT Service Manager is responsible for proposing updates to this policy, which will be reviewed as required but at least annually.
7.3 .The responsibility for ensuring specific line of business information systems are within contract, receive timeous upgrades and are not allowed to become end of life – all of which constitutes a security risk for the Council - lies with the Head of the Service owning/utilising that information system.
7.4 It is your responsibility as an individual to read, fully understand and sign agreement to this policy before access to any ELC resources are given. Please contact ELC's IT Service Desk if advice or guidance is required.

8. Policy Enforcement

8.1 Failure to comply with this policy will lead to the relevant disciplinary procedures being invoked and in certain circumstances actions may be reported to the police or legal action may be taken.
8.2 Any actual or suspected breaches of this policy within, or affecting, the Council's systems will be thoroughly investigated initially by the Head of Corporate Support (or their nominee – normally the Information Security Manager). The employee's line manager will be kept informed of and involved in the investigation. Depending on the circumstances of the breach, there may be a requirement to involve ELC Internal Audit or Police Scotland (if there is a suspicion of criminal activity).
8.3 Breaches of this policy may lead to removal of some services from the employee (i.e. external email, internet access, access to particular systems). Disciplinary action (which will follow the Councils disciplinary procedure) may be taken which could lead to dismissal. Any action taken internally does not preclude prosecution through a court of law. In the event of an issue arising from an interpretation of this policy, it should be resolved by reference to the Head of Corporate Support.
8.4 Reports on activity of users will be produced where requested by appropriate line management (or their authorised depute) where suspected abuses of this policy have been identified.

9. Monitoring and Logging

This policy provides a framework, which if followed, will provide protection against the risks listed in 9.1:

9.1 Uncontrolled use of information systems, the internet and email leaves the Council and its employees open to issues such as, but not limited to:

- Software piracy
- Legal liability (harassment, discrimination defamation etc.)
- Increased risk of system breach via hacking
- The introduction of computer viruses to the Council network
- Downtime and other problems with Council information systems
- Performance problems with the network and internet services
- Potential for legal claims against the Council
- Potential for fines from the Information Commissioner's Office (ICO) if a breach of data protection legislation is found.

9.2 It is recognised that certain groups of staff (including but not limited to Trading Standards, Internal Audit and teaching staff) may require access to internet sites that are normally classified within blocked or restricted web categories. Where legitimate access for work-related purposes is necessary, the staff should contact the IT Service Desk who can arrange for access to be enabled. A business case must be provided and recorded for this access.

9.3 Please note that all monitoring is by automated IT systems. There is no manual interception of, access to or intervention of traffic flows. Exceptions to this will be if a request has been made by a senior manager (or their official depute), or a member of Internal Audit during the course of an official investigation into misuse. Specific members of IT Staff (Infrastructure & Security Team) may have occasion to manually forward emails for business purposes but will only do so following an authorisation process. Mobile devices may use built-in functionality to report the device location to a management system. These records may be used to locate devices in the event of loss or theft but are not used for monitoring staff movement.

9.4 The Council reserves its right to monitor (e.g. content and level of traffic), record, access and/or disclose any messages or data transmitted through the Council's systems in the following circumstances:

Where there is an indication of and to investigate or detect the unauthorized use of Council systems (e.g. breaches of policy and to detect and/or investigate this);
To prevent or detect crime or fraudulent activities;
In specific areas (one being the Contact Centre) voice recording is utilised on the telephony system. These recordings may be used for training and coaching purposes, assisting with the effective dealing of complaints or to take effective action in relation to abusive or threatening phone calls.

9.5 The Council also reserves its right to allow access to email and voicemail accounts, home directories and any other system area, messages or data for the purpose of business continuity. This includes access to email accounts and user folders/files in order to access business communications when a member of staff is on planned or unplanned leave. The Council will endeavour to contact the employee concerned beforehand if possible.

9.6 All users are aware that any transmission through the ELC systems may be accessed by the Council in accordance with this policy, and consequently no user should have any expectation of privacy in connection with their data once transmitted through the systems regardless of whether such transmission has been deleted, or is marked in some manner to indicate that it may be a personal transmission to or from that user.

9.7 In order to ensure that the policy is being followed the Council has in place tools to allow it to filter, monitor and report on the following systems:
Internet access;
Email system;
Telephony systems;
Usage of information systems.

9.8 The Council reserves the sole absolute right to block any website for any reason and to add or remove categories of sites blocked without notice as threats are identified or resolved. The Council will carry out the following automated electronic monitoring, blocking and reporting of internet traffic:

- Access to certain categories of web sites will be restricted and/or blocked. Examples of these include but are not limited to: Adult Material, Drugs, Gambling, Games, Illegal/Questionable, Hacking, Militant/Extremist, Racism/Hate, Tasteless, Violence, Weapons, and Web Chat.
- Access to protocols for downloading files from the internet (such as FTP) will be restricted to specified officers who have a clearly defined business requirement.
- The Council reserves the right to provide reports on usage upon request by an authorised manager, this includes but is not limited to employee usage as part of a suspected breach of this policy or in the event of an investigation into misuse.

The Council will carry out the following automated electronic monitoring, blocking and reporting of external sent and received email traffic in accordance with the impact assessment:

- Check and quarantine or delete messages with attached viruses, trojans and other malicious software (third party system using automated methods)
- Check and reject identifiable spam (third party system using automated methods)
- Check and quarantine encrypted messages or messages with encrypted attachments. (third party system using automated methods)

9.9 Basic information on all calls made through the Council voice (telephony) systems are logged (details logged are source and destination telephone number, date and time of call and duration of call);the Council will carry out this automated electronic monitoring, blocking and reporting of voice traffic.

9.10 Calls made to and from the Council Contact Centre are recorded by an automated voice recording system.

9.11 Evidence of unauthorised use collected during monitoring may be used subsequently in the disciplinary process or during criminal or other investigations. Use of the ELC IT systems constitutes consent to monitoring for these purposes.

Note: Outgoing international calls are blocked on all Council voice systems unless there is a specific business need for this service

10 Use of Systems and Information

The Council's information technology systems and data is provided by ELC only for the purposes of delivering services (and anything associated with those services) to ELC citizens.

10.1 Accessing records on any Council system relating to yourself, a friend, a family member or any other individual which could be construed as a conflict of interest, or getting someone else to access your records may could result in disciplinary action. Where there is a potential conflict of interest, the employee concerned must declare their interest and refer to their line manager.

An employee shall be considered to have a conflict of interest if there exists or potentially exists financial, personal or other interests, which impair their independent and unbiased judgments in the discharge of their duties/responsibilities. Examples of areas where a conflict of interest could take place may include (but not limited to):

- A staff member's personal account;
- Records relating to a relative, friend, neighbour or where the employee has commercial interest.

Any action, or inaction, that may cause detriment, (including but not limited to financial or reputational) to the Council, could be seen as a conflict of interest and failure to declare such an interest could lead to breach of the Council's Disciplinary Code Policy and result in disciplinary action.

10.2 Employees must not use ELC's systems to carry out activities or hold data that is illegal to possess, discriminatory, abusive, offensive, and/or harmful for the Council's interests and breaching the Council's regulations. Such activity would include accessing pornography or violent images. Specifically, pornographic content would include:

- Indecent images of children under 18 which is illegal to possess;
- Obscene materials which it may be an offence to publish but not to possess;
- Materials which is neither an offence to publish nor possess but which some may find distasteful.

10.3 This section is also applicable to all data storage, retrieval, and transfer including web pages, data files and email content.

10.4 The Council acknowledges that user unintentionally may receive inappropriate unwanted emails or redirected to unacceptable websites.

10.5 Users must use only IT resources that are clearly open to and intended for their use e.g. public websites, or websites where the administrator has granted permission.

10.6 ELC systems must not be used for terrorism operations.

10.7 Failure to adhere to any of the above will lead to disciplinary action and/or a potential criminal charge.

11 Council Provided Equipment and Information

The main purpose of this section is to ensure that Council owned IT equipment and media, including all Council software and data/information is used and managed appropriately.

11.1 Sensitive or business confidential information must not be accessible to those not authorised to receive or view it.

11.2 The Council provides equipment, software and information to their employees in order that they may perform their duties in the best interests of the Council. Council equipment must never be connected to any non-ELC equipment or services. The only exception to this would be connection of a Council device to an external Wi-Fi service or telephone carrier network for the purpose of connecting to the ELC infrastructure

11.3 Users of laptops and other portable devices should ensure that where relevant they attach these devices to the ELC network on a regular basis (at least monthly) to enable software updates to be carried out. These tasks occur automatically in the background when the device is connected to the network, or may require you to accept an offered update. This connection can be at an ELC office, or via an external Wi-Fi/mobile service. Each device must be connected for a minimum of 1 hour every month.

11.4 Do not disconnect any device (including cables) connected to an office-based IT asset without IT approval.

11.5 When used outwith Council buildings, all equipment, software and information should be kept secure, confidential and in such a manner as to permit easy access to it by other members of the Council staff when requested.

11.6 Line Managers must approve and document removal of any fixed or shared mobile IT equipment from Council offices.

11.7 As a user of an ELC IT asset you are expected to exercise reasonable control and security over all such equipment, software and data in order to prevent loss, compromise of confidentiality or access difficulties when these resources are needed by other Council staff.

11.8 You must at all times protect your IT Assets from damage, loss or theft.

11.9 Any loss or theft of portable or other equipment or data belonging to ELC should immediately be reported to IT Services through the IT Service Desk.

11.10 Employees should not disclose information relating to the Council's IT facilities to anyone outside the Council. Any telephone canvassing for information should be passed directly to the IT Service Desk.

11.11 No peripheral devices of any kind (digital cameras, printers etc.) may be installed or configured on any Council computer, other than by IT Services. Connecting non-approved equipment can cause configuration issues or disruption to normal IT service. For clarity, this includes personal devices as well as any device not procured by/authorised by the ELC IT service.

11.12 Disposal of IT information assets will be arranged by the IT Services with due regard to legal and environmental issues, ensuring that the appropriate hardware and software registers are updated.

11.13 All IT information assets (including but not limited to: hardware, media, paper etc.) must be disposed of securely following ELC's Data Handling Procedure. The IT Service Desk can provide advice on this.

11.14 ELC business information must not be transferred to any external organisation without first ensuring that:

- There is a valid legal agreement in place (Data Sharing or Data Processing) agreed by the ELC Information Governance team;

- In some circumstances a Data Protection Impact Assessment (DPIA) form may need completed – please seek guidance from the Information Governance team;
- There is a real business need for the transfer;
- The external organisation is aware of their obligations and compliant with the terms of the Data Protection Act or other relevant legislation (if applicable);
- The external organisation has signed the Council's non-disclosure agreement and this has been forwarded to the IT Security Manager;
- Any employee transferring data to an external agency must follow the Councils Data Handling Procedure.

11.15 Only equipment provided by ELC should be used for business purposes. Personal equipment or equipment belonging to third parties should not be used for any work-related activities, or connected to ELC equipment. This includes but is not limited to laptops, digital cameras, tablets, printers, telephones (fixed or mobile) and USB storage devices.

12 Use of PCs and Associated Software including Copyright Issues

It is the policy of the Council to respect all computer software copyrights and adhere to the terms and conditions of any licence to which the Council is a party. The Council will not allow the use of any software that does not have a licence and any user found to be using, attempting to use or in possession of, unlicensed software may be the subject of disciplinary procedures.

12.1 Software Acquisition - All computer software acquired by the Council must be authorised and purchased through IT Services and following correct Council procurement process. Please contact the IT Service Desk for these requests.

12.2 The purchase of software/cloud services or any other IT related asset directly by staff out with IT Services using any other means such as credit cards, expense accounts or petty cash is expressly forbidden.

12.3 Software Delivery - All newly purchased software will be delivered to the IT Services so that licenses can be checked and asset registers updated. No other employee may take delivery of computer software.

12.4 Software Installation - Only IT Services (or their nominee) can install computer software. Under no circumstances is computer software to be installed by any other party without supervision from ELC IT Services.

12.5 Staff Movements - All staff or accommodation moves must involve IT Services so that the appropriate software can be added or removed and/or network connections disabled or made live as appropriate. A moves/changes form (available from IT Service Desk or intranet) must be completed for any such moves.

12.6 Software/Hardware Disposal - Only the IT Services may carry out the disposal of software/hardware.

12.7 Shareware and Freeware – Shareware and freeware software is bound by the same policies and procedures as all software. Only IT Services may install any free or evaluation software onto ELC devices.

12.8 Games and Screensavers -The Council prohibits the use of any games or screensavers other than those installed by default on the PC or Council-provided.

12.9 Auditing - All users should be aware that the Council electronically audits all computers and data on a regular basis. In addition sample random audits may be carried out.

13 Physical Access

All users are responsible for abiding by the following access rules:

13.1 Wear your Staff ID on Council premises and any shared buildings, so that it is visible at all times.

13.2 After finishing work for the day/leaving the office for lunch etc, it is advisable to remove your staff ID badge and keep it secure.

13.3 Ensure any external visitor signs in at reception and is escorted until they leave a Council building or are handed over to another member of staff.

13.4 If you do see someone in a secure area without a Council idenfication badge do not be afraid to ask them to identify themselves. It's important to be vigilant about challenging people you do not recognise as they may have entered the building without authorisation.

13.5 Do not leave external or other secure doors jammed open or unlocked.

13.6 Do not allow others to follow ('tailgate') you into Council buildings unless their staff ID is visible and valid.

13.7 You must close windows when you are the last person leaving a room to prevent unauthorised access to the building.

13.8 Do not allow yourself to be rushed. One person's urgency is not your urgency. Many hacking attempts start by gaining physical access to an organisation's buildings first. These attempts use sophisticated tactics and can be extremely convincing when seeking to gain their way into your office. Social engineers often try to make you feel under pressure in order that you overlook something.

13.9 Always take your time to make informed decisions. Keep calm and use a common sense (if something does not feel right, it probably is not). Always report anything that's doesn't seem right to your line manager or a more senior colleague.

14 Your Desk, Workstation and Documents

The Council recognises that lack of storage facilities in some offices can sometimes mean that data and portable IT hardware and other equipment may be left on employees desks. Whenever possible please take precautions to ensure the security of these items by following the guidelines below.

As we move to use more 'hot desking' facilities it is increasingly important that you do not leave anything behind.

Don't print documents unless you really need to – Council data should whenever possible reside only in the associated information system or central secure file store. This helps not only with keeping our data secure but also with our responsibilities to reduce our environmental impact.

14.1 The Council operates a 'clear desk policy' which means that all desks (even permanent desks) should be cleared at the end of the working day.

14.2 If there is no other option than to leave paper documents and folders on your desk then at least cover any confidential/personal or Council operations information with

another folder or non-confidential documents. Do not leave in clear site of a casual passer-by.

14.3 All confidential items (including documents and digital storage devices) should, wherever possible, be locked in a secure environment when the area is unattended.

14.4 No information of a confidential nature should be available for casual viewing or inspection by visitors.

14.5 IT devices should not be left unattended in an unlocked state where unauthorised individuals could access applications or documents or systems.

14.6 All filing cabinets, cupboards and safes that contain confidential material should be locked when unattended. The keys for these items should be stored in such a way as to maintain security, but also to allow access in the event of your absence.

14.7 All confidential documents should be disposed of securely. Under no circumstances should Council confidential information be disposed of in rubbish bins or waste paper recycling containers. The majority of our offices should now have access to a confidential waste disposal container. Documents placed in these containers are securely destroyed. If you do not have access to secure disposal, please request this through your line manager.

14.8 All confidential documents that have been sent to a shared printer/device without card-controlled secure printing facility should be collected immediately and not left for casual viewing or inspection.

15 Passwords

Passwords provide the first line of defence against unauthorised access to your computer and our Council's infrastructure and data. The stronger your password, the more protected we will be from hackers and malicious software. You should maintain strong passwords for all your work accounts.

15.1 All ELC IT users are given a username and password ('credentials') to control access to Council systems; these are unique and **must not** be revealed to anyone else. Treat your username and password as you would your bank card pin number.

15.2 Never log another user on to the system using your username and password. You may be held responsible for any activity that happens using your credentials and this could lead to disciplinary action against you.

15.3 Credentials should not be written down, stored in a computer file, or kept where others might find them. The exception to this is if you are using KeePass, ELC's encrypted password manager database. KeePass is installed on all ELC devices, if you are unsure how to use it please ask the IT Service Desk for advice.

15.4 Passwords should be hard to guess (not just a normal word you might find in a dictionary) and contain at least twelve characters, including upper case, lower case, numeric and special characters (such as ! # £ $). Try using a passphrase instead - Passphrases and Multi-Factor Authentication - Stay Safe Online

15.5 The IT Service Desk will assist in demonstrating how to change your password if you are unsure how to do this but want to. Our network systems are configured to force password changes annually.

15.6 As an authorised user of ELC IT infrastructure you are responsible for the security of your passwords and user accounts.

15.7 If at any time you think someone may have discovered your password you must immediately change it or request that it is changed and report this to the IT Service Desk.

15.8 If a user has forgotten their password, it will be necessary for the password to be changed by the IT Service Desk. In these cases proof of identity will be required as for account/password creation.

15.9 You must never use the 'remember/store password' facility on a system/website.

16 Access Control

16.1 It is a criminal offence under the Computer Misuse legislation to deliberately attempt to access or modify a system to which you have no authority.

16.2 The IT department monitors ELC systems and unauthorised access attempts are logged and investigated.

16.3 All Council data/information should be saved on central server storage on or the associated business system. This ensures Council data is secured and backups are performed regularly. Data/information saved directly to laptop drives, virtual desktop environments such as Citrix or any other endpoint devices is not backed up.

16.4 Removable media devices should not be used for transferring or storing confidential data. These devices include but are not restricted to:
Optical media such as CDs or DVDs; USB storage (memory sticks, portable hard disks); flash memory cards (such as XD and SD cards) and mobile phones.

16.5 Any transfer of data must be handled using a platform supporting a process and encryption level approved by IT Services and our Data Protection Officer. Please read the Council's Data Handling policy for detailed guidance.

17 Email Acceptable Use

These systems are an invaluable business tool for the Council. In order to ensure that they are used appropriately it is important that staff note the following:

17.1 Emails have the same legal status as written documents so the same degree of care must be taken. Emails should be considered the same as a written letter or memo.

17.2 Always double check the recipient address line before sending a message and check it is being sent to the correct person (sending to the wrong recipient is one of the most common forms of data breach).

17.3 Never represent yourself as another person or persons.

17.4 Delete electronic mail messages when they are no longer required to ensure we meet our Data Protection and records management requirements.

17.5 External emails are automatically appended with an ELC-approved disclaimer.

17.6 Suspicious email attachments from unknown senders must not be opened as they may contain viruses, fraudulent offers, malicious computer code or any other form of malware. Always contact IT Services via the IT Service Desk for advice if unsure in this situation.

17.7 Users should exercise caution when opening files attached to emails. These attachments can contain viruses, executable files or other such information, which may breach copyright laws or contain a destructive payload.

17.8 If an employee feels that they are being/have been harassed via the email system they should seek to address the issue through the appropriate policies of the Council. There may be circumstances where a complaint will be investigated and action, in accordance with the appropriate disciplinary procedure, taken.

17.9 If an employee feels a defamatory statement has been made in relation to them via the email system they should seek to address the issue through the appropriate policies of the Council.

17.10 The Council provides the email system to assist users in the performance of their duties and therefore its main use should be limited for official business. However, incidental and occasional personal use of email is permitted by the Council.

17.11 Personal use of the email system should never impact the normal traffic flow of business related email. The Council reserves the right to purge identifiable personal email to preserve the integrity of the email systems.

17.12 Take care not to express views, which could be regarded by others as offensive or libellous. Comments made in jest may be interpreted differently by a recipient.

17.13 No user should use the Council's email system in any way that may be interpreted as insulting, disruptive or offensive by any other person, or Council, or which may be harmful to the Council's reputation. This includes the forwarding any email sent to you by somebody else.

17.14 Examples of prohibited material include but are not limited to: Sexually explicit messages, images, cartoons, or jokes; requests for dates, or love letters; profanity, obscenity, defamation of character or libel; tthnic, religious, or racial slurs; political

beliefs or commentary (unless connected with Council business); or any other message that could be construed as harassment or disparaging of others based on their sex, race, sexual orientation, age, national origin, disability, religious or political beliefs.

17.15 You should be aware that all emails sent or received through the Council's email system will automatically be placed in an archive in line with the Freedom of Information Act 2002 after 60 days unless the email has been deleted by the user. Any email in the archive may be opened and read during either a FOI request or an investigation into misuse.

17.16 Users are not permitted to receive software via email. All software must be purchased through the IT Services.

17.17 No messages should be sent or received which could be construed as inciting unlawful activities.

17.18 The use of external and web based email systems (e.g. Yahoo mail, Hotmail) are strictly prohibited on the corporate network.

17.19 Council data/information must not be sent from or to your personal email account.

17.20 The use of instant messaging products or similar is also not permitted outwith those specifically authorised and made available by IT Services.

17.21 The forwarding of chain letters is strictly forbidden. This includes those purporting to be for charity or other good causes as well as those promising wealth or other personal gain.

17.22 No unsolicited messages of any kind should be sent to multiple external destinations. This may be considered as 'spamming' which is an illegal activity. An exception to this rule may be emails that are sent to a group of people for a legitimate business reason.

17.23 Email is not always a secure form of communication. Messages that you send may transfer over networks owned by other people. If you require a high level of security for an email you should check with IT Services for advice before sending.

17.24 The user logged in to a device or session will be considered the author of any messages sent from that device or session. Remember to log out from/lock/shutdown (as appropriate) any device or session that will be left unattended. Under no circumstances should you send email from a device or session logged into by another user.

17.25 Email addresses should not be disclosed unnecessarily. If you provide your address when filling in surveys or other questionnaires you will be at risk of receiving unwanted junk messages.

17.26 Users should be wary when subscribing to email lists, and should avoid this if possible. Advice on this can be obtained from the IT Service Desk. The volumes of messages that can be generated are high and you have little control over the content. This may bring you into conflict with other conditions stated within this policy.

17.27 Email should not be used to send large attached files. Many email systems will not accept large files, resulting in non-delivery. IT Services should be consulted prior to sending any messages over 20MB in size.

17.28 In no circumstances should any facility to automatically forward emails/calendar entries etc. be used to forward items to personal email accounts, or any other email account outwith the ELC environment. This would breach our code of connection agreement with the Government Public Services Network, and poses a high level of information security risk.

17.29 Your Council-supplied email address should not be used to sign up to websites for personal use. These include but are not limited to: personal purchasing via the web, e.g. eBay, Amazon, holiday booking sites, social networking sites such as Facebook etc.

17.30 Do not forward mail messages to other individuals or groups that have been sent to you containing personal data (as defined by the Data Protection Act 2018) without the permission of the originator.

17.31 Forwarding email – don't forward long email trails without removing previous data, only forward the content that is useful to the conversation. Forwarding emails trails could potentially end up with data being sent to the wrong person and put us at risk of a data breach.

17.32 Report any unusual or suspect email messages to IT Service Desk.

17.33 If you are sending an email to a lot of recipients from different organisations, use the BCC field to protect their email addresses from others.

18 Internet Acceptable Use

The Council will provide access to the Internet to all authorised users to assist them in the performance of their Council duties.

18.1 Where access is provided, use should be limited to official Council business during working hours (i.e. during periods when staff are recording themselves as at work) Personal use of the Internet is permitted but must be out-with working time.

18.2 No messages, images or any other type of information, (including the use of East Lothian Council's name) should be posted on any internet message board or other similar web-based service, social networking site or any other website that could bring the Council into disrepute, or which a reasonable person would consider to be offensive or abusive.

18.3 Identification methods exist, including the address of the computer you are using, which may still allow others to locate the Council that you work for, and the particular computer used to post a message. As part of our routine security measures, all websites visited are centrally logged.

18.4 Users should not engage in any activities which could be deemed to be illegal whilst using an ELC provided internet connection.

18.5 The system may not be used for personal financial gain, nor should you host a personal website on any Council equipment or systems.

18.6 Your use of the system should not have a noticeable effect on the availability of the system for other users. Therefore you should not participate in online games or have active any web channels that broadcast frequent updates to your PC (e.g. internet radio, 'as live' TV or films etc.) unless required as part of your job.

18.7 Users should not visit websites that display material of a pornographic nature, or which contain material that may be considered offensive. It is recognised that you may accidentally view such material, if this happens please contact the IT Service Desk immediately.

18.8 Users should not download any software or copyrighted material from internet sites. If you require software downloaded from a website please contact IT Services – they will ensure an appropriate assessment of any such software is completed. Where there is a clearly defined business requirement access to protocols for downloading files from specific Internet sites (such as SFTP) may be allowed.

18.9 You must logout from or lock your device if it will be left unattended. Under no circumstances should you browse the internet from a device logged into by someone else. It may be a disciplinary matter if you fail to log out of or lock a device when not in use.

18.10. Users must not attempt to access illicit or unlawful web sites.

18.11 The use of web-based remote access tools is strictly prohibited. Remote access to the Council network is strictly controlled. Users should also not use third party sites or services to access their home computers from the Council network. These sites and services include but are not limited to: LogMeIn, TeamViewer, Webex, GoToMyPC, VNC. The use of peer-to- peer sites and software is also prohibited.

18.12 Access to the Internet is filtered. Where a user has a legitimate need to access blocked sites they should log a call with the IT Service Desk, giving a business case for access.

18.13 As well as job-related use, the internet may also be used for the following purposes during normal working hours with the relevant line manager's consent: to assist with a recognised course of study, CPD or academic research; for personal development or for accessing a Council-approved computer based learning course. Note: there is no access to third party web-based email systems via the corporate network even for this exception.

18.14 The Council monitors and logs all Internet access by individuals and reserves the right to access and report on this information.

19 Remote working/Mobile computing

The Council now encourages homeworking where agreed with a line manager or remote working from shared buildings or from other locations using your Council equipment and systems. This policy applies no matter where you are based at any time. Whatever the location there must be due regard to the terms of this policy and in particular due regard to data protection particularly when transferring and storing data.

19.1 Do not store Council data on the hard drive of a portable device, always store on a central server shared folder. Our remote working laptops connect to our central systems as long as you have access to WiFi or your device has a SIM card. Contact the IT Service Desk for advice.

19.2 Use a suitable carry case when transporting your laptop or other portable device. This will keep it dry, protect it from damage and make it a less obvious crime target.

19.3 Do not leave the device lying visibly in your car or in a public place. Make sure you keep it secure at all times when out of the office.

19.4 Never store passwords with the equipment.

19.5 If you use your device at home do not leave it where it is accessible by others.

19.6 If you leave the portable device at the office keep it in a locked cupboard or drawer overnight where possible.

19.7 Remote workers must ensure their laptop and any other portable devices are updated as required. Out of date devices pose a high risk to the Council's infrastructure security and may be suspended from connecting if allowed to become too out of date with requirements. More information on updates can be found in section 11.3.

19.8 Do not connect any found or gifted cables, memory sticks or other USB devices to a USB port on any ELC device (sometimes marketing campaigns gives USB sticks and cables for free).

19.9 Do not discuss confidential matters in public places.

19.10 If you are using your device in a public place or on public transport, make sure that no one can read the data on your screen over your shoulder.

20 Mobile and Fixed Line Phones

19.1 The Council supplies mobile phones to members of staff where it is required to assist in the delivery of their duties.

19.2 When using a Council mobile phone, the Council Mobile Phone Acceptable Use Policy (issued on receipt of a Council phone) should be signed and adhered to.

19.3 All personally owned mobile devices (mobile phones, PDAs, media players etc) or any other device capable of storing data are prohibited from being used in connection with your position at ELC, and may not be attached to Council systems or information assets.

21 Encryption

Encryption is when a document, email or data is protected to make the contents unreadable to anyone who does not have the password or encryption key.

20.1 No Council data should be encrypted by password, without the password being held in a secure store such as KeePass. It is then the line manager's responsibility to ensure that the password is looked after to the extent that other people may access the data in the event of absence.

20.2 No encryption software may be used on Council systems without the prior approval of the Head of Corporate Support. In the event of approval being given, a copy of the encryption key should be submitted to the IT Service Desk

20.3 No emails should be sent out with the Council domain using any standalone encryption service without the prior approval of the Head of Corporate Support. Encrypted emails without this approval will be blocked by IT Services.

20.4 Encryption software may only be purchased and installed by the IT Services.

22 Biometric Data

Biometric data is information about an individual's external physical characteristics, such as fingerprints or retina pattern. You may already use this to unlock your ELC iPhone. At this moment in time ELC does not retain any biometric data, if you do use your fingerprint to unlock your Council iPhone this data is stored directly on to the device and ELC has no access.

ELC reserves the right to use and retain biometric data in the future for the purposes of delivering its services if required.

23 Disclaimer

East Lothian Council accepts no responsibility for the malfunctioning of any equipment or software, failure in security or integrity of any stored program or data, or for any loss alleged to have been caused, whether by defect in the resources or by act of neglect of ELC or its employees.