Computers, Internet, and E-Mail Policy

V1.0 January 2026

Introduction

ELCAP's IT and communications systems are intended to promote effective communication and work practices.

This policy sets out basic rules regarding the use of ELCAP electronic equipment, software, email and internet use. It outlines standards you must observe, explains when we will monitor use, and the action we will take if you breach standards.

It is your responsibility to ensure you understand and comply with all the rules in this policy, as failure to comply could, depending on the violation, result in disciplinary action including dismissal, and notification to the appropriate authorities for criminal/civil proceedings.

This policy does not form part of any contract for work or employment and we may amend it at any time.

Our Business Manager has overall responsibility for this policy, including keeping it under review.

1. Equipment security

ELCAP electronic 'equipment' (this may may include computers, laptops, any handheld devices such as mobile phones, iPhone or iPad), and also any work email, systems, internet and associated facilities ("facilities") made available are primarily for work purposes.

All use of equipment and facilities will be subject to monitoring, as described in this policy.

ELCAP may allow personal use on the basis and on the understanding that such use may be withdrawn at any time. Personal use, if permitted, is only allowed during your break times or before or after working hours.

You are responsible for the security of the electronic equipment allocated to or used by you. You must not allow anyone else to use that equipment other than in accordance with this policy.

You must use passwords on all equipment, particularly items that you take out of the office.

Equipment should not be removed from our premises without authorisation. Where you have use of portable equipment, it is important to maintain a high level of security and care. This is to ensure that there is no unauthorised access.

You must follow the Company's back-up procedures specific to portable equipment to ensure that information is saved and stored securely.

You must not attach any device or equipment including mobile phones, tablet computers or USB storage devices to our systems without authorisation from our Business Manager, in consultation with our IT provider.

If an item of portable equipment is lost or damaged due to an act of negligence, the individual responsible may be liable to contribute to the cost of replacement or repair.

You must install current antivirus and malware protection on any personal device or computer used for work, and comply with our instructions relating to software security and to implement all updates to equipment as soon as you are requested to do so.

Inform our Business Manager immediately if you suspect your equipment may have a virus or malware.

2. Protocol for using ELCAP facilities

All staff with an email account must enable Two-Factor Authentication (2FA) to ensure security. This requires a code to be entered when logging back into an account or when a password is changed or updated.

Company policy prevents log in to your devices or accounts from outside the UK. Should you require access while outside the UK, you must request permission directly from Business Manager ahead of the travel and this will be authorised and the policy suspended or the required period of time

You must only log on to our facilities and systems using your own username and password. You must not use another person's username and password or allow anyone else to log on using your username and password.

For reasons of data security and recoverability, all documents, spreadsheets and other computer files should be saved to the appropriate folders on the server/SharePoint. You must adhere strictly to this policy, as files saved to an individual's equipment might not be backed up and the information will be lost in the event of a computer crash, which constitutes an unlawful data breach. You should consult your Line Manager if you are in any doubt about where to save and store files.

You should not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of your duties).

Downloading unauthorised software may interfere with our systems and may introduce viruses or other malware. You must not download or install software from external sources without authorisation from our Business Manager. It is strictly prohibited, both by law and under this policy, to copy any licensed software to or from the Facilities. Duplication of a licensed product, regardless of whether it is purchased, is a breach of such licence and may be viewed as gross misconduct.

Data should never be downloaded or printed unless it is for work.

If you are away from your desk, you should log out or lock your equipment.

At the end of each working day, you must log out and shut it down.

You must share data only through our designated secure messaging applications or our online document sharing system, Egress, or via encrypted emails. All work-related calls are to be made through our designated video-conferencing softwares, which are Microsoft Teams, Google Meet and Zoom.

Teams meetings and document uploads via the Microsoft Teams Application must be confirmed with privacy setting and not public before sharing documents.

In order to protect confidential information, it is forbidden for photographic equipment to be used on our premises outside of work purposes, without the written permission of [Business Manager]. This includes mobile phones with camera function, camcorder, webcams, tape or other recording device for sound or pictures, whether moving or still. If there is any doubt as to whether a device falls into this category, advice should be sought from the Manager who will clarify the matter.

Under no circumstances should any meeting or conversation be recorded without the knowledge and permission of all present.

3. Protocol for Password-Protected Documents / Sending Sensitive Documents

Identify Sensitive Content

- Clearly identify documents that contain sensitive information, such as criminal offence records or special category data.

Password Protection Strategy

- Before sending any sensitive documents via email, they must be encrypted or secured with a strong password.
- Use reliable software tools (like Microsoft Office or Adobe PDF) that allow you to set a password for documents.

Share Passwords Securely

- Never include the password in the same email as the sensitive document.
- Instead, share the password using a different communication method (e.g., text message, phone call, or secure messaging app – typically egress within local authorities).

Limit Access

- Share sensitive documents only with individuals who absolutely need to see them. Maintain an access log if appropriate.

4. Passwords

Ensure your email account is protected with a strong, unique password that includes a mix of letters, numbers, and symbols, as explained below:

- Length

Aim for at least 12-16 characters. Longer passwords are generally more secure.

- Complexity

Use a mix of upper and lower case letters, numbers, and special characters (e.g., !, @, #, $, %).

- Avoid Common Words

Don't use easily guessed passwords such as "password," "123456," or personal information like your name or birthday.

- Passphrases

Consider using a passphrase made up of random words or a sentence that is easy for you to remember but difficult for others to guess.

- Unique Passwords

Use different passwords for different accounts to avoid a breach affecting multiple accounts. Store your passwords securely using a password manager if needed

You must keep your passwords confidential and change them regularly. Make sure that your password and username are not visible on your device to avoid anyone accessing without permission and compromising your account or ELCAP data.

Never use a password that is easily guessed or broken (e.g. not your name or date of birth, or a family member name, etc).

Never share your password with anyone

5. **E-mail access and use**

Email remains a primary mode of communication within ELCAP for sharing both generic and sensitive information, including documents related to criminal offences or special category data.

Due to the risks associated with email correspondence, it is crucial to adopt robust data protection practices to safeguard sensitive data from unauthorized access and breaches.

By following these best practices for data protection, combined with compliance with our policies and procedures, ELCAP can greatly reduce the risk of unauthorised access to sensitive information transmitted via email. It is essential for all staff members to remain vigilant and adhere to these protocols whenever sending or handling sensitive documents.

<u>Use Secure Email Services</u>

- Our organisation has security measures in place that are supported by our external IT teams.
- Our accounts are password protected and have two point authentication in situ for all devices. Access to devices also include pin passwords for additional security.

<u>Verify Recipients</u>

- When communicating via email, it is best practice to draft your email before adding any recipients. This ensures that the content can be reviewed before sending, spelling and grammar can be checked and minimises the risk of sending an email with uncleansed information.
- Always confirm the recipient's email address before sending and email, especially when it includes sensitive information.
- Consider using phone calls or instant messaging to verify the receipt of an email if this is warranted.
- E-mail addresses are private and personal information. They should not be disclosed to any person without proper reason for doing so.

Care should be taken with content of emails. Adopt a professional tone and observe appropriate etiquette when communicating with third parties by email. Before sending, an email should be checked carefully for grammar and spelling errors, in the same way that a paper document would be checked before sending. You should also include our standard email signature and disclaimer.

Emails should not be distributed to people who have no need to receive them. Care should also be taken not to overload people with unnecessary emails. There is a banner policy that identifies external recipients and incoming emails which should be checked before responding or sending

Remember that emails can be used in legal proceedings and that even deleted emails may remain on the system and be capable of being retrieved. They must therefore never contain anything that is unprofessional or could damage our reputation.

In particular, you must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate emails. What may be intended as a joke could cause offence to others. The Company will not tolerate the sending or forwarding of any messages that could constitute bullying or harassment as identified in the Anti-Bullying, Harassment & Stalking Policy.

You should not:

- send, forward or read private emails at work which you would not want a third party to read;
- send or forward chain mail, junk mail, cartoons, jokes or gossip;
- contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding emails to others who do not have a real need to receive them; or
- send messages from another person's email address (unless authorised) or under an assumed name.

Untrue statements made about a colleague, or third party, even intended as a joke, can be viewed as defamation, harassment, or slander and could result in you and/or the organisation being sued.

Do not use your own personal email account to send or receive emails for work purposes. Due to the non-secure nature of Internet email, you must consider Internet email to be public information. No confidential information should be transmitted over the Internet.

If the origin of a received email is not known, you must not reply to it or forward it to other people. If there are any attachments, these must not be opened in any circumstances, and all instances must be reported to Management.

Before opening other incoming email attachments from known recipient, you must first use the virus screening software provided.

Personal emails should be kept to the essential minimum in the same way as personal phone calls should be treated. You should note that these may be monitored as detailed in this policy. If, for work reasons, you need to send Company information to your personal email address, you should first notify your line Manager.

6. **Internet access and use**

Internet access is provided primarily for work purposes.

You should not access any webpage or download any image or other file from the internet which could be regarded as illegal, offensive, discriminatory, in bad taste or immoral. Even web content that is legal in the UK, it may be in sufficient bad taste to fall within this prohibition.

As a general rule, viewing a webpage will be a breach of this policy if:

- any person (whether intended to view the webpage or not) might be offended by its contents; or
- the fact that our software has accessed the webpage or file might be a source of embarrassment if made public.

We will not tolerate the use of the Internet for illegal or inappropriate activities. Such activities include (but are not limited to):

- online gambling
- accessing offensive, obscene or indecent material, including pornography
- downloading or distributing copyrighted information
- sending or posting abusive, rude or defamatory messages or statements about people or the organisation

You are not permitted to load or run unauthorised games or software, or to open documents or communications from unknown origins.

Information on the internet is likely to be protected by copyright. No information from the internet should be used in any business publications or other material without the source and related copyright being checked by management.

We may block or restrict access to some websites at our discretion.

7. **Personal use of our equipment and facilities**

We permit the incidental use of our systems to send personal email, browse the internet and make personal telephone calls, subject to certain conditions.

Personal use is a privilege and not a right. It must not be overused or abused. We may withdraw permission for it at any time or restrict access at our discretion.

Personal use must meet the following conditions:

- it must be minimal and take place [substantially OR exclusively] outside of normal working hours (that is, during your lunch break, and before or after work);
- personal emails should be labelled "personal" in the subject header;
- it must not affect your work or interfere with work;
- it must not commit us to any marginal costs; and
- it must comply with our policies, including this policy

You are permitted to access personal web logs (blogs) or social networking sites on the internet whilst at work but only during non-working hours i.e. before or after work, or during recognised break periods. However, you are still expected to adhere to certain standards of conduct to be observed to protect both its legitimate business interests and its employees from the dangers of inappropriate use. These are:

- You must not post information on your personal blog or any social networking sites which is confidential to the organisation, its staff, its service users or customers.
- You must not post entries on the organisation's blog or your personal blog or any social networking sites which are derogatory, defamatory or offensive in any way, or which could bring the Company into disrepute or be offensive to work colleagues.
- You must always be aware of your duty to act in good faith and in the best interests of the organisation. We will not tolerate criticisms posted in messages in the public domain or on blogs about us or any other person connected to us.
- You should be aware that blogs or social networking site entries may create documents which the courts can order to be disclosed for use in litigation. Consequently, you will be assumed to have written any contentious items unless you can prove definitively that you have not done so.
- Any blog entries or social networking site entries made inside or outside the workplace that are defamatory, derogatory or discriminatory about the Company, its employees, its suppliers or customers, will be subject to disciplinary action in accordance with this policy
- The Company will monitor its IT systems as is believed necessary to prevent inappropriate usage. Hard copies of blog or social networking site entries will be used in any disciplinary proceedings.

8. **Monitoring**

Our systems enable us to monitor equipment and facilities, including telephone, email, voicemail, internet and other communications. Our External IT provider have deployed security and monitoring policies to ensure safety of all accounts.

For security and for operational reasons, and in order to carry out legal obligations in our role as an employer, your use of our systems, including any personal use, may be continually monitored by automated software or otherwise for the following purposes:

- To comply with any legal obligation
- To protect confidential information and personal data entrusted to us
- To ensure legitimate use of the systems
- To fulfil our legal obligations to ensure that staff do not access or communicate obscene, offensive, illegal or inappropriate material including anything which could amount to harassment or bullying, and to assist in the investigation of alleged wrongdoing
- To retrieve messages lost during a system failure or lost for any other reason
- To ensure that personal use does not adversely impact on work performance
- For training purposes and to address any service issues or complaints.

This list is not exhaustive.

We reserve the right to retrieve the contents of email messages or to check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the organisation.

Nothing stored, sent or received on the Facilities is private from ELCAP. Nor is the identity of its source or destination. You should be aware that the data that you create on the Facilities remains the property of ELCAP and may require to be accessed in your absence to ensure continuity of service.

You should note that the Company may require to access, reproduce, disclose or delete any material. If necessary the Company will inform you of this in advance, however, in certain circumstances, the Company can legally access, reproduce, or disclose or delete any material without your consent (e.g. if it is suspected that a crime is being committed or if it is suspected that there is an issue which could result in disciplinary action being taken)

9. **Prohibited use of our systems**

Misuse or excessive personal use of our telephone or email system or inappropriate internet use will be dealt with under our Disciplinary Procedure. Misuse can in some cases be a criminal offence.

Creating, viewing, accessing, transmitting or downloading any of the following material will usually amount to gross misconduct (this list is not exhaustive):

(a) pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);

(b) offensive, obscene or criminal material or material which is liable to cause embarrassment to us or to our clients or customers;

(c) a false and defamatory statement about any person or organisation;

(d) material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches our Diversity, Equity and Inclusion Policy or our Anti-harassment and Bullying Policy);

(e) confidential information about us, our business, or any of our staff, clients or customers (except as authorised in the proper performance of your duties);

(f) sending, receiving, downloading, displaying or disseminating material that insults, causes offence or harasses others

(g) engaging in on-line chat rooms or gambling

(h) posting inappropriate comments in personal blogs or social networking sites

(i) forwarding electronic chain letters or similar material

(j) downloading or disseminating copyright materials

(k) downloading or playing computer games and

(l) unauthorised or unlawful copying or downloading of software

Please note that this is not an exhaustive list.