Extend Learning Academies Network (ELAN)
Staff, Volunteers and Visitors Acceptable Use Policy 2026-27

This document is part of the ELAN ICT and Online Safety Policy

Trust Policy

ELAN will ensure that staff and volunteers have good access to digital technology to enhance their work and enable efficient and effective working. In return, staff and volunteers will be expected to agree to be responsible users.

Scope of Policy

This Acceptable User Policy (AUP) applies to staff and volunteers who have access to and are users of the ELAN's ICT systems and to work related use of ICT systems outside of their main place of work.

General Responsibilities

Staff, volunteers and visitors who have access to and are users of ELAN's ICT systems are expected to:

- Read, understand, sign and act in accordance with the ELAN ICT and Online Safety policy and Data Protection policy
- Use ELAN's ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users
- Report any illegal, inappropriate or harmful material, data breaches, suspected misuse or concerns about the use of ICT to a senior leader or Trust CEO
- Model the safe use of ICT
- Refrain from publishing any information that: may be offensive to colleagues, may breech the integrity of the ethos of ELAN or may bring the trust into disrepute (this includes personal sites)
- Protect own professional identity online by ensuring security settings for social networking sites are enabled fully
- Ensure acceptable use of social media
- Respect copyright.

Phones and devices in school

NOTE: Any reference to devices within this document refers to: iPad / tablet / laptop / mobile phone / all devices with imaging and sharing capabilities / USB devices.

ELAN staff personal phones / devices

- Staff are not permitted to use personal phones / devices while pupils are present.
- Staff personal phones / devices should be locked away in school during pupil contact time.
- Staff use of personal phones / devices is restricted to non-contact time, and to designated areas of the school such as the staff room and offices where pupils are not present.
- Personal phones / devices should not be used to take photographs or recordings of pupils, their work, or anything else which could identify a pupil.
- In the event of a personal mobile needing to be used for work related activity such as two-factor authentication with pupils present, this should be done with transparency and supervision of another member of staff present prior to the device being securely stored.
- If access to a personal phone / device is required in the classroom for medical purposes, this will be with the full knowledge and agreement of the senior leadership team and will remain locked and secure away from pupil access. The phone / device will never be accessed when pupils are present except in circumstances of medical emergency. Personal phone / devices could be subject to monitoring and review by the senior leadership team.
- Personal phones and devices should not be used to download or store school or trust information/data. If there is a need to download information in exceptional circumstances, this should be deleted from the device as soon as possible. In the event that information is downloaded in error, it should be deleted immediately. Access to online platforms is limited to Microsoft 365 and should be through an internet browser and not an app.

ELAN work phones / devices

- Some members of staff are provided with a phone or device by ELAN central team or school for work purposes 'a work phone / device'.
- Only authorised staff are permitted to use work phones/devices, and unsupervised access to those devices must not be provided to anyone without trust authorisation.
- Work device functions must only be used for work purposes; this includes making/receiving calls; sending/receiving emails; two-factor authentication; app use; internet use; camera use or any other communication.
- Staff must ensure that all use, communication and conduct linked to a work phone / device is transparent, appropriate and professional, and adheres to the ELAN staff code of conduct and trust policies.
- Staff visiting an ELAN school site with a designated work phone / device are not required to surrender the work phone / device on arrival. Staff should inform the school that a work phone / device is being carried and why this is needed on their person during the visit.
- Whilst on the school site the work phone / device should not be visible and placed on silent/vibrate. If there is a need to use the work phone / device whilst on a school site, this should be done within a designated safe place and where pupils are not present.
- Staff visiting an ELAN school site with a work phone / device should inform the school on arrival of any potential need to use the device to take photos during the visit and its purpose.
    - Prior to taking pictures that include pupils, staff must ask the school to identify any pupils that cannot be photographed.
    - A member of the school staff or trust colleague should be in attendance during camera use where pupils are present as this negates any potential issues or allegations.
    - The Trust/school has the right to check any images taken / stored on a work phone / device. Best practice dictates that staff should show the school all images taken during their visit prior to leaving.
    - Any photos that include pupils or images that identify pupils should be deleted from a work phone / device once transferred to other trust media/storage or when no longer required.
    - Photos should never be transferred to personal devices or memory sticks.

Volunteers, contractors' (and anyone else otherwise engaged by the school) phones / devices

- All persons visiting an ELAN school must surrender phones/devices on arrival in line with the school's procedures unless there is a legitimate business reason for not doing so. Examples of legitimate business reasons are, but not limited to: building condition photography, to provide a quotation for works, two-factor authentication, logging work undertaken on site.
- The person visiting must seek approval from a senior leader if they have a legitimate business reason to carry a phone/device on the school site.
- Where permission is granted for a phone/device to be carried on the school site, either
    - The person visiting will need to be escorted by a member of staff (this can be any member of staff employed by ELAN) for the duration of the visit.
    - Or where the person visiting cannot be escorted or it is not practicable, they will be required to either:
        - agree before commencing activity on site that they will share their phone/device for checking camera roll prior to leaving site Or
        - use a phone/device provided by the school whilst on site.

Visitors' phones / devices

- All persons visiting an ELAN school must surrender personal phones / devices on arrival in line with the school's procedures.

ELAN Microsoft 365 accounts

- Microsoft 365 services are provided to ELAN employees/volunteers to support the organisation's primary purposes of education and its associated business functions.

- Accounts are used to access emails, Teams and the Staff Portal in addition to other services provided by Microsoft.

Email monitoring

- ELAN reserves the right to access employee email accounts, records and content of emails sent and received by employees where it is necessary for legitimate business purposes, for the investigation of allegations of improper use or behaviour or to investigate alleged contraventions of any of the organisation's rules, regulations, policies and procedures, where it can be shown to be necessary and proportionate.
- Email accounts may also be accessed for the purposes of crime prevention and detection, the apprehension or prosecution of offenders or for actual or prospective legal proceedings or for the purposes of exercising, establishing or defending legal rights.
- Where account access is required, there would be two members of senior leadership present and all activities logged.

Third party access to email

- Where an employee/volunteer is absent from work for an unexpected or prolonged period, ELAN reserves the right to grant access to their email account for business continuity purposes.
- Access will normally be granted to the employee/volunteer's line manager. A record will be kept of the access granted, the reasons and duration of access.
- As soon as it is practicable and appropriate, the user of the email account will be notified.
- Where access is granted to an employee/volunteer's email account under these circumstances, it will be made clear that emails marked as, or appear to be, private or personal must not be opened or forwarded and must be treated confidentially.

Retention and deletion of email accounts

- When an employee or volunteer leaves ELAN, their email account and network access will be disabled from the date of their last working day.
- Where there is an identified business need, ELAN reserves the right to grant access to an employee/volunteer's email account and files for a period of time after the leaving date. Access will normally be granted to the employee/volunteer's line manager. A record will be kept of the access granted, the reasons and duration of access (see model log sheet).
- Employees/volunteers are encouraged to delete any personal emails, such as payslips, pensions correspondence, from the email account before their leaving date and to notify the pension provider of an alternative email address.
- The email account will be fully deleted once the retention period has passed as defined in ELAN's email retention schedule. This will trigger the complete purge of the mailbox after another 30 days.

Technical Infrastructure

Staff, volunteers and visitors who have access to and are users of ELAN's ICT systems should not try to by-pass any of the technical security measures that have been put in place by the trust. These measures include:

- the proxy or firewall settings of the trust network (unless permission has been granted)
- not having the rights to install software on a computer (unless permission has been granted)
- not using removable media (unless permission has been granted)

Passwords

Staff, volunteers and visitors who have access to and are users of the ELAN's ICT systems should ensure that:

- Username and passwords are not shared with anyone else and are protected from unauthorised disclosure.
- Passwords are stored securely. Passwords should not be written down or stored in a way that they could be accessed by someone else.
- The same password must not be used across different accounts or applications.
- Default passwords must be changed.

Filtering and Monitoring
ELAN uses Smoothwall filtering and monitoring. The use of ELAN's ICT, digital technology and communication systems will be monitored. Staff, volunteers and visitors who have access to and are users of ELAN's ICT systems should ensure that:

- They do not try to by-pass the filtering system used by the trust (unless permission has been granted).
- If special access is granted to sites that are normally filtered, the computer / device should not be left unsupervised.
- Any filtering issues should be reported immediately.
- Smoothwall monitor is installed on all school/work devices and is active at all times, regardless of location. It monitors activities on these devices, looking for keywords, phrases, or other indicators that might suggest a risk or concern. As part of the Smoothwall monitor reporting, screen captures are taken of the relevant window before and after a potential risk has been identified.

Online professional and personal safety
Staff, volunteers and visitors who have access to and are users of ELAN's ICT systems are expected:

- To be aware of the Trust's ICT and Online Safety Policy and adhere to its guidelines.
- To be professional in all communications and actions at all times when using ELAN's ICT systems. Communications should not use aggressive or inappropriate language.
- To not engage in any on-line activity that may compromise professional responsibilities.
- To only use chat and social networking sites in work in accordance with the Trust's policies.
- To only communicate with pupils, parents/carers, and colleagues using official trust/school systems. All communication should be professional in tone and manner.
- To be aware of the risk of using personal email addresses, mobile phones and social networking sites for such communications.

Cyberbullying

- ELAN has a zero tolerance of bullying. In this context cyberbullying is seen as no different to other types of bullying.
- Any incidents of bullying should be reported in accordance with trust procedures.

Digital Images
Staff, volunteers and visitors who have access to and are users of ELAN's ICT systems are expected:

- To ensure that when taking and/or publishing images of others, it is done so with the individual's permission and in accordance with the ELAN's policy on the use of digital / video images.
- To not use personal equipment to record images, unless permission has been given to do so. Where these images are published (eg on the trust website) it should not be possible to identify by name, or other personal information, those who are featured.

System and Data Security
Staff, volunteers and visitors who have access to and are users of ELAN's ICT systems are expected:

- To not access, copy, remove or otherwise alter any other user's files, without their express permission.
- To not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted. Any concerns about the validity of an email should be reported immediately due to the risk of the link or attachment containing viruses or other harmful programmes.
- To ensure that data is regularly backed up, in accordance with relevant ICT policies.
- To not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. To not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- To not try (unless permission has been given) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- To not install or attempt to install programmes of any type on a machine, or store programmes on a computer, or try to alter computer settings (unless permission has been given).
- To not disable or cause any damage to trust equipment, or the equipment belonging to others.
- To ensure personal devices are protected by up to date anti-virus software and are free from viruses when using them in work or when visiting another ELAN site.
- To only transport, hold, disclose or share personal data in accordance with the ELAN Data Protection Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- To keep all staff, pupil, parent/carer data private and confidential, except when it is deemed necessary or required by law or by trust policy to disclose such information to an appropriate authority. Any disclosure of information must be in accordance with ELAN's Data Protection Policy (or other relevant policy).

The Use of Artificial Intelligence (AI) Tools and Technologies

Staff, volunteers and visitors who have access to and are users of ELAN's ICT systems are expected:

- To ensure that they use AI in line with the ELAN Use of Artificial Intelligence (AI) Policy
- To ensure that they use AI and emerging technologies responsibly to minimise the risk to safety, privacy, or security of ELAN's systems and in line with the ELAN Use of Artificial Intelligence (AI) Policy. To only use AI tools and technologies approved by the trust for purposes authorised by the trust and ensure compliance with data protection laws when handling personal data.
- To only use trust-provided AI accounts for work purposes. These accounts are configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.
- To ensure that any sensitive or personally identifiable information about staff, pupils, parents/carers is only entered into AI systems that have explicit approval and robust security measures in place.
- To not upload sensitive information, such as internal documents into third-party AI tools unless approved by the trust for that purpose.
- To report any incidents involving AI misuse, data breaches, or inappropriate outputs immediately to a senior leader or the trust CEO.

Copyright

Staff, volunteers and visitors who have access to and are users of ELAN's ICT systems are expected:

- To ensure that they have permission to use the original work of others in their own work.
- To not download or distribute copies (including music and videos) of any work that is protected by copyright.

Training

Staff, volunteers and visitors who have access to and are users of ELAN's ICT systems are expected to:

- Participate in ICT, online safety, cyber security and GDPR training on an annual basis.
- Participate in any other training where there is an identified knowledge or skills gap.

Reporting Incidents

- Any illegal, inappropriate or harmful material, data breaches, security incidents, suspected misuse or concerns about the use of ICT should be reported immediately to a senior leader or the trust CEO.
- Any incidents should be recorded in accordance with ELAN procedures.
- In some cases the Police may need to be informed.
- Any suspicious emails that could represent a cyber-threat should be reported to a senior

leader/line manager immediately

- Any damage or faults involving equipment or software should be reported to a senior leader.

Sanctions and Disciplinary Procedures

- Any misuse of the Trust ICT systems may result in disciplinary procedures.

Staff, Volunteers and Visitors
Acceptable Use Policy Declaration 2026-27

I have read and understand the above and agree to use ELAN's ICT systems (both in and out of my place of work or when visiting another site within the trust) and my own devices (in my place of work or when visiting another site within ELAN and when carrying out communications and actions related to the trust) within these guidelines or any additional guidelines set by the trust.

I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to the trust CEO/Directors and in the event of illegal activities the involvement of the police.

Staff/Volunteer/Visitor Name _____

Signed _____

Date _____