Extend Learning Academies Network (ELAN)
Staff, Volunteers and Visitors Acceptable Use Policy 2023-24

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

Trust Policy

The Trust (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 Trust's ICT systems and to work related use of ICT systems outside of their main place of work.

My Responsibilities

I agree to:

- Read, understand, sign and act in accordance with the ELAN ICT and Online Safety policy and Data Protection policy
- Use school 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
- Should I require access to my personal device 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. This device will never be accessed when pupils are present except in circumstances of medical emergency. I understand that my personal device could be subject to monitoring and review by the senior leadership team.
- Refrain from publishing any information that: may be offensive to colleagues, may breech the integrity of the ethos of the Trust 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
- 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

I understand that:

- 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, this should be done with transparency and supervision of another member of staff present prior to the device being securely stored.

ELAN work phones / devices

I understand that:

- Some members of staff are provided with a phone or device by the Trust 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

I understand that:

- All persons visiting an ELAN school must surrender phones/devices on arrival in line with the school’s procedure 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

I understand that:

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

Training

- I understand that I will participate in ICT, online safety, cyber security and GDPR training
- I understand that it is my responsibility to request training if I identify gaps in my abilities.

Cyberbullying

- I understand that the Trust has a zero tolerance of bullying. In this context cyberbullying is seen as no different to other types of bullying.
- I understand that I should report any incidents of bullying in accordance with Trust procedures.

Technical Infrastructure

I will 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 I have permission)
- not having the rights to install software on a computer (unless I have permission)
- not using removable media (unless I have permission)

Passwords

- I will only use the password(s) given to me
- I will never log another user onto the system using my login
- I will not disclose my username or password to anyone else
- I will not try to use any other person's username and password.
- I will not write down or store a password where it is possible that someone may steal it.

Filtering

- I will not try to by-pass the filtering system used by the Trust (unless I have permission)
- If I am granted special access to sites that are normally filtered I will not leave my computer unsupervised
- I will report any filtering issues immediately
- I understand that the Trust will monitor my use of the Trust's ICT, digital technology and communication systems.

ELAN email accounts

I understand that:

- Office365 email services are provided to ELAN employees/volunteers to support the organisation's primary purposes of education and its associated business functions.

Email monitoring

I understand that:

- 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

I understand that:

- 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

I understand that:

- 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.

I will be professional in my communications and actions when using Trust ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the Trust's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the Trust website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in work in accordance with the Trust's policies. I will have read the Trust's ICT and Online Safety Policy and adhere to its guidelines.
- I will only communicate with students / pupils and parents / carers using official Trust systems. Any such communication will be professional in tone and manner. I am aware of the risk of using my personal email addresses, mobile phones and social networking sites for such communications.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The Trust have the responsibility to provide safe and secure access to technologies:

- When I use my own personal mobile devices in work or when visiting a school, I will follow the rules set out in this agreement, in the same way as if I was using equipment owned by the Trust. I will also follow any additional rules set by the Trust about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant ICT policies.
- I will 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. I will

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.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings (unless I have permission).
- I will not disable or cause any damage to Trust equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Trust 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.
- I understand that data protection policy requires that any staff or student/pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by Trust policy to disclose such information to an appropriate authority. This needs to be transferred securely. E.g. Via Egress/ password protected.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for Trust sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions within and outside my place of work:

- I understand that this Acceptable Use Policy applies not only to my work and use of Trust ICT equipment within my place of work, but also applies to my use of Trust ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment 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.

Reporting Incidents

- I will report any illegal, inappropriate or harmful material, data breaches, suspected misuse or concerns about the use of ICT to a senior leader or the Trust CEO.
- I will make a note of any incidents in accordance with Trust procedures.
- I understand that in some cases the Police may need to be informed.

Sanctions and Disciplinary Procedures

- I understand that if I misuse the Trust ICT systems in any way then there are disciplinary procedures that will be followed by the Trust.

Staff, Volunteers and Visitors
Acceptable Use Policy Declaration 2023-24

I have read and understand the above and agree to use the Trust 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 the Trust and when carrying out communications related to the Trust) within these guidelines.

Staff/Volunteer/Visitor Name _____

Signed _____

Date _____