

Acceptable Use Policy (AUP) Agreement - Staff

Introduction

Technologies that have become integral to the lives of our learners, both at school and in their lives outside school, can stimulate discussion and promote creativity, promoting effective learning. They also bring opportunities for staff to be more creative and productive in their work.

The Trust aims to ensure that staff and volunteers have good access to IT to enhance their work and improve opportunities for learners and, in return, expect staff and volunteers to agree to be responsible users.

This Acceptable Use Policy (AUP) Agreement is intended to ensure:

- That staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- That Trust/Academy IT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff and volunteers are aware of the General Data Protection Regulation (GDPR), comply with the rules it sets out and follow the training and advice given.

For my professional and personal safety:

- I understand that the Trust will monitor my use of Trust/Academy IT systems, email and other digital communications. This may include, but not be limited to, the following circumstances:
 - With software to monitor 'trigger' words or phrases for safeguarding and to ensure acceptable, professional use of IT. Any concerning behaviour by staff or volunteers will be detected automatically, alerting both Trust/Academy DSLs.
 - When staff leave or are on long-term absence for retrieval or redirection of messages.
 - When a member of staff is under investigation or suspected of illegal, fraudulent, inappropriate or safeguarding activity.
 - To collect and review information contained in any electronic system for documented purposes and authorised by the Principal/CEO, for example, to complete a Subject Access Request or similar.
- I will comply with the Trust Online Safety Policy, LwLAT AI Policy and LwLAT Social Media Policy.
- I understand that the rules set out in this agreement also apply to use of Trust/Academy based IT systems on laptops, email, iPads, etc outside of work.
- I understand that the Trust/Academy IT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the Trust.
- I will keep my usernames and passwords private and will not use anyone else's username and password.

- I will not share or continue to use any logins for any Trust or Academy service or platform when I leave my employment.
- I will return all Trust/Academy owned IT equipment and delete all Trust or Academy data from my personal devices when I leave my employment.
- I will not attempt to repair or move any IT equipment myself, and will report the issue to IT Services.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the Principal/CEO or IT Services.

I will be professional in my communications and actions when using Trust/Academy IT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate in a professional manner at all times.
- 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.
- I will only use chat and social networking sites at work in accordance with Trust policies.
- I will only communicate with learners and parents/carers using official Trust or Academy systems.
- I will not share any personal information with a learner (including personal phone numbers or email address).
- I will not request or respond to any personal information from a learner unless it is appropriate as part of my professional role, and with explicit permission to do so.
- I will report any attempt by a learner to make contact with me personally to a DSL.
- I will not engage in any on-line activity that may compromise my professional responsibilities.
- I will lock my screen or log off my computer when I leave it unattended.
- I will not allow a third party to access my work emails on a personal device, such as my mobile phone or tablet.
- If the data on any device is compromised or a breach takes place, I will report it to IT Services immediately.

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

- When using personal hand held/external devices (iPads/laptops/mobile phones etc) at work, I will follow the rules set out in this agreement, in the same way as if I was using Trust/Academy owned equipment.
- I will also follow any additional rules set by the Trust about such use. As far as I am able, I will ensure that when connecting these devices to Trust/Academy IT systems, they are using up to date Operating Systems (e.g. latest versions of Android / iOS) and are protected by up to date anti-virus software where applicable.
- I will not save any personal work data to a personal computer or device.
- I will not use my personal WhatsApp accounts to share organisational data, such as learner data, staff information, or any other confidential work-related details.
- I will only use the recommended apps on my personal device for accessing data\emails via Office 365.
- I will encrypt (e.g. password protect) my personal device if I use it to access personal work data via Office 365, or equivalent apps.
- I will inform the Principal/CEO/IT Services if my personal device e.g. laptop, phone or tablet is lost or stolen should it contain any personal work data.
- I will immediately report any Internet content that is not filtered that I suspect could be inappropriate.
- I will delete personal data according to the Trust Retention Policy.
- I will not use personal email addresses for work-related purposes.
- I will ensure that my data is regularly backed, in accordance with relevant Trust policies.
- I will not open any attachments in unexpected emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes. I will alert IT Services of any suspicious activity.
- I will not upload, download or access any material which is illegal or inappropriate or may cause harm or distress to others (e.g. child sexual abuse images, criminally racist material, adult pornography etc).
- 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 install or attempt to install programmes of any type on Trust/Academy systems, or alter computer settings, unless this has been explicitly authorised by the Principal, CEO or IT Services.
- I will not disable or cause any damage to Trust/Academy equipment, or 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. Where personal data is electronically transferred outside the secure Trust network, it must be encrypted.
- I will immediately report any damage or faults involving equipment or software, however this may have happened, to IT Services.

Using the internet in my professional capacity or for school 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).

Use of Electronic Whiteboards and Screensharing:

- I understand that electronic whiteboards should be used in a manner that upholds the Trust's standards of professionalism and respect.
- I will ensure that any content displayed or written on electronic whiteboards during lessons or meetings is appropriate for the intended audience.
- I will not save or store personal or sensitive information displayed on the whiteboard without the necessary permissions or safeguards in place.
- When using interactive features, I will ensure that learner data and privacy are protected at all times.
- When sharing the screen of my device (laptop, tablet, work phone etc) to the electronic whiteboard, I will ensure that only the necessary applications or windows are visible to avoid unintentionally sharing sensitive or personal information. This also applies to screensharing during online remote lessons or meetings.
- I will be vigilant and ensure that any notifications or pop-ups that may contain personal or sensitive information are disabled before sharing my screen to the electronic whiteboard, or during online remote lessons or meetings.
- I will ensure that any shared content displayed on the electronic whiteboard or shared during online remote lessons or meetings, upholds the Trust's standards of professionalism and respect.

Use of the Management Information System (MIS):

- I understand that the Academy/Trust MIS contains sensitive data and information pertinent to the functioning of the Academy/Trust.
- I will only access the MIS with the appropriate permissions and for legitimate work-related purposes.
- I will not share my MIS login credentials with anyone and will ensure that I log out after each session.
- I will ensure that I do not display or share information from the MIS with individuals that are not authorised the access the data (for example, by displaying the MIS on classroom screens or electronic whiteboards).
- I will immediately report any suspected breaches or unauthorized access to the MIS to IT Services.
- I will use multi-factor authentication, where available, to enhance the security of my access to the MIS.

Use of Safeguarding System (CPOMS, SignIn Central Record)

- I acknowledge the sensitive nature of data within Trust/Academy safeguarding systems and will handle this information with utmost care and discretion.
- I will ensure that I only access these systems for legitimate safeguarding-related activities and will avoid unnecessary browsing or querying of data.
- I will not share my login credentials for safeguarding systems with anyone.
- I will ensure that I do not display or share information from the a safeguarding system with individuals that are not authorised the access the data (for example, by displaying the information on classroom screens or electronic whiteboards).
- Multi-factor authentication should be used when accessing these systems to ensure the highest level of security.
- Any suspected breaches, mishandling, or unauthorized access to these systems should be reported immediately to a Designated Safeguarding Lead.

I understand that I am responsible for my actions in and out of work:

- I understand that this Acceptable Use Policy Agreement applies not only to my work and use of Trust/Academy IT equipment in work, but also applies to my use of Trust/Academy IT systems and equipment outside of work and my use of personal equipment in work or in situations related to my employment with the Trust/ Academy.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action possibly resulting in a 6-month/12-month warning that will remain on my personnel file and be included in any references, a suspension from duties, dismissal, a referral to the LADO, a referral to the DBS or a referral to the TRA (Teaching Regulatory Standards), where appropriate, and in the event of illegal activities, the involvement of the police.

I have read and understand the above and agree to use Trust/Academy IT systems both in and outside of work and my own devices (in work and when carrying out communications related to the Trust/Academy) within these guidelines.