

EPA Trust – Staff, Directors, Governors & Visitors
ICT Acceptable Use Policy (AUP)



THIS POLICY WAS AGREED BY TRUSTEES ON (Date):	August 2026
REVIEW DATE:	August 2027
CHAIR OF TRUSTEES:	
CEO:	

Contents

1.Introduction Scope and Aims	2
2.Relevant Legislation and Guidance	2
3.Definitions	3
4.Unacceptable Use	3
4.1 Exceptions from Unacceptable Use.....	5
4.2 Sanctions	5
5. Staff (Including Directors, Governors, Volunteers and Contractor)	5
5.1 Access to Trust ICT Facilities and Materials.....	5
5.1.1 Use of Phones and E-Mail.....	5
5.2 Personal Use	6
5.2.1 Personal Social Media Accounts	7
5.2.2 Artificial Intelligence (AI)	7
5.3 Remote Access.....	7
5.4 Trust Social Media Accounts.....	7
5.5 Monitoring of Trust Network and Use of ICT Facilities.....	7
6. Data Security	8
Passwords	8
Software Updates, Firewalls and Anti-Virus Software	9
Data Protection	9
Access to Facilities and Materials	9
7. Internet Access	9
8. Monitoring and Review.....	10
9. Related Policies	10
Annex 1: Social Media Guidelines.....	11
Annex 2: Acceptable Use Agreement for Staff, Directors, Governors, Volunteers and Visitors.....	12

1. Introduction Scope and Aims

ICT is an integral part of the way our organization works, and is a critical resource for staff, directors, governors, volunteers and visitors. This policy sets out the acceptable use of ICT resources by Staff within the EPA Trust, directors, governors, visitors or contractors. It applies when working at the Trust's main site, remotely, or any school within the Trust. Staff must also comply with individual school ICT and safeguarding policies when on-site.

This policy aims to:

- Set guidelines and rules on the use of ICT resources for staff, directors, governors, volunteers and visitors.
- Establish clear expectations for the way all members of the organization engage with each other in respect to ICT systems.
- Supports any relevant policy on data protection, online safety and safeguarding.
- Prevent disruption to the organization through the misuse, or attempted misuse, of ICT systems.
- Breaches of this policy will be treated in the same way as any other misconduct issue and ultimately could result in dismissal. Illegal activities will be reported to the police and, if necessary, the Oxfordshire Safeguarding Children Partnership (OSCP).

The Trust recognises that technology plays an increasingly important role in safeguarding children. All users of Trust ICT systems are expected to use technology safely, responsibly and professionally, recognising that online behaviours may present safeguarding concerns. This policy supports the Trust's safeguarding responsibilities under *Keeping Children Safe in Education 2026* and should be read alongside the Child Protection and Safeguarding Policy.

2. Relevant Legislation and Guidance

This policy refers to, and complies with, the following legislation and guidance:

- [Data Protection Act 2018](#)
- [The General Data Protection Regulation](#)
- [Computer Misuse Act 1990](#)
- [Human Rights Act 1998](#)
- [The Telecommunications \(Lawful Business Practice\) \(Interception of Communications\) Regulation 2000](#)
- [Investigatory Powers Act 2016](#).
- [Education Act 2011](#)
- [Freedom of Information Act 2000](#)
- [The Education and Inspections Act 2006](#)

- [Keeping Children Safe in Education 2026](#)
- [Meeting Digital and Technology Standards in Schools](#)
- [Filtering and Monitoring Standards for schools and Colleges](#)
<https://www.gov.uk/government/publications/working-together-to-safeguard-children--2>
- [Searching, Screening and Confiscation: Advice for Schools](#)

3. Definitions

“ICT facilities” / “Trust’s ICT network” : Includes all facilities, systems and services including but not limited to network infrastructure, cloud hosted systems, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service. This can apply both onsite and offsite.

“Users”: Anyone authorised by the Trust to use the ICT facilities, including staff, directors, governors, volunteers and visitors.

“Personal use”: Any use or activity not directly related to the users’ employment, study or purpose.

“Authorised personnel”: Employees authorised by the EPA Trust to perform systems administration and/or monitoring of the ICT facilities.

“Materials”: Files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs.

4. Unacceptable Use

The following is considered unacceptable use of the EPA Trusts ICT facilities by any member of the Trust. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the Trust’s ICT facilities includes:

- Using the Trust’s ICT facilities to breach intellectual property rights or copyright.
- Using the Trust’s ICT facilities to bully or harass someone else, or to promote unlawful discrimination.
- Breaching the Trust’s policies or procedures.
- Any illegal conduct, or statements which are deemed to be advocating illegal activity.
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate.
- Activity which defames or disparages the Trust, or risks bringing the Trust into disrepute.
- Sharing confidential information about the Trust, its staff, students, or other members of the Trust community.
- Connecting any device to the Trust’s ICT network without approval from authorised IT personnel.

- Setting up any software, applications or web services on the Trust's ICT network without approval by authorised IT personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data.
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised IT personnel.
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the Trust's ICT facilities.
- Causing intentional damage to ICT facilities.
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel.
- Causing a data breach by accessing, modifying, losing, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation.
- Using inappropriate or offensive language.
- Promoting a private business, unless that business is directly related to the Trust.
- Using websites or mechanisms to bypass the Trust's filtering mechanisms.
- Take or store images of staff or students on personal devices, including mobile phones and tablets.
- Staff must not create, possess, distribute or knowingly access AI-generated indecent, manipulated or deepfake images involving children or adults connected with the Trust.
- Staff must not knowingly access, create or share misogynistic, extremist or other harmful online content using Trust ICT systems.
- Any concerns relating to AI-generated abuse, deepfakes or harmful online content must be reported immediately to the Designated Safeguarding Lead (DSL).
- This is not an exhaustive list. The Trust reserves the right to amend this list at any time. The Trust's Leadership Team or school's leadership, if necessary, will use professional judgement, or seek legal advice, to determine whether any act or behaviour not on the list above is considered unacceptable use of the Trust's ICT facilities.

4.1 Exceptions from Unacceptable Use

Exemptions to the policy may be granted at the CEOs discretion and each must be agreed prior to use.

Examples of exceptions for unacceptable use are:

- ICT staff using or working with external organisations for the purpose of penetration testing or bypassing filters to check network security, with prior approval.
- Installing applications or web services that support teaching and learning, with additional authorisation from the Trust's IT department.
- Compliance with legal requirements or to protect the health, safety, or welfare of students and staff.

4.2 Sanctions

Staff who engage in any unacceptable activity listed above may face disciplinary action in line with relevant Trust's policies on behaviour, discipline and Code of Conduct and, if necessary, reported to the police or the Oxfordshire Safeguarding Children Partnership (OSCP).

5. Staff (Including Directors, Governors, Volunteers and Contractor)

5.1 Access to Trust ICT Facilities and Materials

The Trust's IT Department and Managed Service Providers manage access to the Trust's ICT facilities and materials for Trust staff. That includes, but is not limited to:

- Computers, laptops, tablets and other devices.
- Access permissions for Trust resources such as programmes or files.

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the Trust's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the Director of IT, CEO or a member of the Trust IT Department or Managed Service Provider

5.1.1 Use of Phones and E-Mail

The Trust provides each member of staff with an email address. This email account should be used for work purposes only. All work-related business should be conducted using the email address the Trust has provided. Staff must not share their personal email addresses with parents and student and must not send any work-related materials using their personal email account.

Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.

Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All

email messages should be treated as potentially retrievable.

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error which contains the personal information of another person, they must inform the Director of IT, CEO or a member of the Trust or School leadership team immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or students. Where provided, Staff must use phones issued by the Trust to conduct all work-related business.

Trust phones must not be used for personal matters.

Staff must report any AI safeguarding concerns.

5.2 Personal Use

Staff are permitted to occasionally use Trust ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The CEO, Trust leadership team or Director of IT and Trust IT Team may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not constitute 'unacceptable use' as defined in section 4.
- Takes place when no students are present.
- Does not interfere with their jobs or prevent other staff or students from using the facilities for work or educational purposes.

Staff may not use the Trust ICT facilities to store personal non-work-related information or materials (such as music, videos, or photos).

Staff should be aware that use of the Trust's ICT facilities for personal use may put personal communications within the scope of the Trust's ICT monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff should be aware that personal use of ICT (even when not using Trust ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where students and parents could see them.

Staff should take care to follow the Trust or visited Schools guidelines on social media (see annex 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal Social Media Accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times.

The Trust has guidelines for staff on appropriate security settings for Facebook accounts (see annex 1).

5.2.2 Artificial Intelligence (AI)

The Trust recognises that Artificial Intelligence (AI) can support learning and administrative tasks when used responsibly. Staff must ensure that any use of AI is lawful, ethical and in line with safeguarding, data protection and copyright requirements.

Staff must:

- only use Trust-approved AI platforms where available
- never enter confidential, personal or safeguarding information into public AI tools
- never upload pupil work, assessments or personal data into AI systems unless authorised
- ensure AI-generated content is checked for accuracy before use
- maintain professional judgement and not rely solely on AI-generated responses
- comply with GDPR, copyright and intellectual property requirements
- Staff must immediately report any concerns relating to AI-generated abuse, deepfakes, manipulated imagery or other online safeguarding concerns to the Designated Safeguarding Lead

5.3 Remote Access

We allow staff to access their individual work areas, shared areas and ICT facilities remotely.

Staff accessing the Trust's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the Trust's ICT facilities outside the Trust and take such precautions against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Staff working remotely must ensure devices are securely locked when unattended, avoid using public Wi-Fi unless connected via an approved secure connection, and take reasonable steps to prevent unauthorised viewing of confidential information.

The Data Protection policy can be found on the Trust website and in the Staff Shared Area.

5.4 Trust Social Media Accounts

For any instances of the Trust utilising an agreed social media account. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The Trust may post guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

5.5 Monitoring of Trust Network and Use of ICT Facilities

The Trust reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity/access logs
- Any other electronic communications

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

The Trust monitors ICT use in order to:

- Obtain information related to Trust business.
- Investigate compliance with Trust policies, procedures and standards.
- Ensure effective Trust and ICT operation.
- Conduct training or quality control exercises.
- Prevent or detect crime.
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation.

The Designated Safeguarding Lead (DSL) will work with the Director of IT, Trust IT Team and managed service providers to ensure filtering and monitoring systems are appropriate for the age and needs of pupils, are reviewed annually, and that any alerts relating to safeguarding concerns are acted upon promptly. Staff should report any concerns regarding the effectiveness of filtering and monitoring systems to either the DSL, Trust IT Team including managed service providers or Director of IT.

6. Data Security

The Trust takes steps to protect the security of its computing resources, data and user accounts. However, the Trust cannot guarantee security. Staff who use the Trust's ICT facilities should use safe computing practices at all times.

6.1 Passwords

All users of the Trust ICT facilities should set strong passwords for their accounts and keep these passwords secure. These should meet the following requirements:

- 12-character minimum length
- Not a single dictionary word.
- Different passwords used between email and other systems, e.g. MIS platform, curriculum software and any personal accounts. Using the same password can significantly weaken security and must not be done.

A good example of a strong password would be: **Purple!River9Laptop2**

Where multi-factor authentication (MFA) is available it must be enabled. This can be through Single Sign on technologies.

Users are responsible for the security of their passwords and accounts, and for setting permissions for

accounts and files they control.

6.2 Software Updates, Firewalls and Anti-Virus Software

All of the Trust's ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the Trust's ICT facilities.

Any personal devices using the Trust's ICT network must all be configured in this way.

Staff should remain vigilant to phishing emails, QR code scams, malicious links and other cyber security threats and report any suspected incidents immediately, to the DSS, Director of IT or Trust IT Team including Managed service providers.

6.3 Data Protection

All personal data must be processed and stored in line with data protection regulations and the Trust's data protection policy. Staff must not upload confidential Trust information, safeguarding records, personal data or pupil work to publicly available AI platforms or unapproved cloud storage services.

6.4 Access to Facilities and Materials

All users of the Trust's ICT facilities will have clearly defined access rights to Trust systems, files and devices.

These access rights are managed by Director of IT, or Trust IT Team including managed service providers.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the CEO, Trust leadership team or Director of IT and Trust IT Team immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed completely at the end of each working day.

7. Internet Access

Internet access within the Trust is protected with an approved filtering system. This filtering system will provide an appropriate level of protection to staff, students and visitors. If you identify a site that is not being filtered appropriately you should inform the Director of IT, Trust IT Team, or Managed Service Provider as a matter of urgency. It may also be appropriate to contact the Trust or School Leadership Team. If you feel that a site has been filtered in error, please report the issue to allow a review to take place. Across the Trust the schools have wireless networks that solely provides access to the internet.

Staff must not give the wifi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

8. Monitoring and Review

The CEO, Director of IT and Director of Safeguarding will monitor implementation of this policy to ensure it remains compliant with statutory safeguarding, cyber security and data protection requirements. This policy will be reviewed every 1 year in July to allow for a September adoption.

9. Related Policies

This policy should be read alongside the Trust policies on:

- Data Protection Policy
- Privacy Policy

Annex 1: Social Media Guidelines

Don't accept friend requests from students on social media

- Facebook, Twitter, Snapchat, Instagram, TikTok, YouTube, LinkedIn are examples of social media sites.
- Staff should ensure that the privacy settings of their social media accounts are set so that only friends can view posts.
- Social media sites should be used responsibly and professionally.
- Staff must not communicate with pupils via personal social media accounts or private messaging platforms.
- Staff should not use social media sites in such a way that damage might be caused to the reputation of the Trust.
- Defamatory comments should not be made on social media sites.
- Members of staff should be aware of copyright rules, and should not place copyright material on social media sites without permission of the copyright owner.
- Staff should think carefully about the consequences of anything they write or send within social media sites.
- All members of staff must abide by the Data Protection principles. Third party personal data (e.g. of students) should not be placed on the internet / social media sites. This includes photo's with names.
- Other confidential or sensitive or financial information should not be placed on social media sites.
- Misuse of social media sites may be investigated under disciplinary procedures.
- Remember, there is potential for anything you post online to be copied and distributed. Bear this in mind every time you post.

Annex 2: Acceptable Use Agreement for Staff, Directors, Governors, Volunteers and Visitors

Acceptable Use of the Trust's ICT Facilities and the Internet: Agreement for Staff, Directors, Governors, Volunteers and Visitors	
Name of staff member/director/governor/volunteer/visitor:	
When using the Trust's ICT facilities and accessing the internet across the organisation, or outside it on a Work or personal device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material). • Use them in any way which could harm the Trust's reputation. • Access social networking sites or chat rooms. • Use any improper language when communicating online, including in emails or other messaging services. • Install any unauthorised software, or connect unauthorised hardware or devices to the Trust's network. • Share my password with others or log in to the Trust's network using someone else's details. • Share confidential information about the Trust, its students or staff, or other members of the community. • Access, modify or share data I'm not authorised to access, modify or share. • Promote private businesses, unless that business is directly related to the Trust. • Store any confidential or personal data on external devices such as USB hard drives or personal PC's, laptops or tablets. • I will not upload confidential Trust or pupil information into public AI platforms. • I understand AI-generated information must always be checked before use. • I will immediately report AI-generated indecent imagery, deepfakes or online safeguarding concerns to the DSL. • I understand that misuse of AI may be treated as a disciplinary matter. • I will report any cyber security incident or suspected phishing attack immediately. • I understand that AI is intended to support, not replace, my professional judgement.	
I understand that the Trust will monitor the websites I visit and my use of the Trust's ICT facilities and systems. I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside the Trust, and keep all data securely stored in accordance with this policy and the Trust's data protection policy. I will let a school's designated safeguarding lead (DSL) and the Trust Director of IT know if a staff member or student informs me, they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the Trust's IT systems and internet responsibly and ensure that students in my care do so too. Note: Governors and Directors may sign this form by way of a confirmation on Governor Hub	
Signed (staff member/director/governor/volunteer/visitor):	Date: