PolyMAT

Acceptable Use Policy & Agreement for Staff, Governors, Volunteers & Visitors

Reviewed: November 2023

Approved: December 2023

Revision due: December 2024

Acceptable Use Policy and Agreement

This policy is designed to enable acceptable use for staff and governors (Trustees and Academy Committee Members).

The Trust provides a range of ICT resources which are available to staff members and governors. In order to ensure the safety of staff, governors and pupils it is important that all staff members and governors follow the guidelines detailed below.

This policy aims to:

- Promote the professional, ethical, lawful and productive use of the Trust's ICT systems and infrastructure;
- Define and identify unacceptable use of the Trust's ICT systems and external systems;
- Educate users about their data security responsibilities;
- Describe why monitoring of the ICT systems may take place;
- Define and identify unacceptable use of social networking sites and Trust devices; and
- Specify the consequences of non-compliance.

This policy applies to staff members, governors and all users of the Trust's ICT systems who are expected to read and understand this policy. To confirm acceptance of the policy, users will sign an Acceptable Use Agreement which is attached to this policy. Breach of this policy may result in disciplinary action.

The use by staff and monitoring by the Trust of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the Data Protection Act 2018, together with the Employment Practices Data Protection Code issued by the Information Commissioner. Staff are referred to the School's Data Protection Policy for further information.

If you are in doubt and require clarification on any part of this document, please speak to the Data Protection Lead for your setting and/ or the Trust Network Manager.

Provision of ICT Systems

All equipment that constitutes the Trust's ICT systems is the sole property of the Trust.

No personal equipment should be connected to or used with the Trust's ICT systems. Users must not try to install any software on the ICT systems without permission from the Trust Network Manager. If software is installed without permission, it may cause extensive damage to the ICT systems and users could be held personally liable for any costs incurred in rectifying the damage.

The Trust Network Manager is responsible for purchasing and/or allocating ICT equipment to individuals. Individual laptops/desktop computers or ICT equipment may be removed at any time and without prior warning for regular maintenance, reallocation or any other operational reason. Maintenance includes but is not limited to, new software installations, software updates, reconfiguration of settings and computer re-imaging.

Network Access and Security

Users are not permitted to make any physical alteration either internally or externally, to the Trust's computer and network hardware.

All users of the ICT systems across the Trust must first be registered. Following registration, a network user account will be created consisting of a username, password and an e-mail address. All passwords should be of a complex nature to ensure data and network security. All user account details are for the exclusive use of the individual to whom they are allocated. Staff are responsible for ensuring their password remains confidential and their account is secure. Passwords must be regularly changed.

All users are personally responsible and accountable for all activities carried out under their user account(s). Users must take all reasonable precautions to protect their user account details and must not share them with any other person, except to designated members of the IT Support team for the purposes of system support. Users must report any security breach or suspected breach of their network, email or application account credentials to the Trust Network Manager as soon as possible.

Users should only access areas of the Trust's computer systems to which they have authorised access.

When any computer is left unattended, it must either be logged off or locked. Activity that threatens the integrity of the Trust's ICT systems or activity which attacks or corrupts other systems, is forbidden. Users' internet activity must not compromise the security of the data on the Trust's ICT systems or cause difficulties for any other users.

Trust Email

Under no circumstances should a pupil be allowed to use a staff computer account, unless being directly supervised by the account owner at all times.

Where email is provided, it is for academic and professional use with reasonable personal use being permitted. Personal use should be limited to short periods during recognised break times and comply with this Acceptable Use policy. The Trust's email system can be accessed from both the Trust's computers and via the internet from any computer. Wherever possible, all Trust/ school related communication must be via the Trust email address.

The sending of emails is subject to the following rules:

- Language must not include swear words, be offensive or abusive.
- Emails or attachments of a pornographic, illegal, violent, sexist or racist nature are not permitted.
- Sending of attachments which contain copyright material to which the School does not have distribution rights is not permitted.
- The use of personal email addresses by staff for any official school business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g., sensitive or personal information) will only be sent using a secure method including:
  - Email encryption;
  - A secure upload portal (where by the recipient will be required to log in to retrieve the email/documentation sent);
  - Password protection on sensitive documents. The sender must ensure that the password is sent separately to the intended recipient (i.e., in a separate email or over the phone).
- Emails should not contain children's full names in the subject line and preferably, not in the main body of the text either. Initials should be used wherever possible.
- Access to school/setting email systems will always take place in accordance to data protection legislation and in line with other appropriate school/setting policies e.g., confidentiality.

- Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the relevant files/records (such as safeguarding).
- Staff will be encouraged to develop an appropriate work life balance when responding to email.
- Emails sent to external organisations should be written carefully and checked before sending, in the same way as a letter written on school headed paper would be.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Where possible, emails must not contain personal opinions about other individuals e.g., other staff members, children or parents. Descriptions of individuals must be kept in a professional and factual manner.

Further details about how to use the Trust's ICT systems for communication can be found in the Electronic Information and Communication Policy and the Internal Communications Policy and Protocols.

Internet Access

Internet access is provided for academic and professional use with reasonable personal use being permitted. Priority must always be given to academic and professional use.

The Trust's internet connection is filtered meaning that a large amount of inappropriate material is not accessible. However, on occasions it may be possible to view a website which is inappropriate for use in a school. In this case, the website must be reported immediately to the IT Support Team.

Therefore, staff must not access from the Trust's system any web page or any files downloaded from the web which could be regarded as illegal, offensive, in bad taste or immoral.

Misuse of the internet may in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material or using any of the following facilities will amount to gross misconduct (this list is not exhaustive):

- accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;
- transmitting a false and/or defamatory statement about any person or organisation;
- sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive, derogatory or may cause offence and embarrassment or harass others;
- transmitting confidential information about the Trust and any of its staff, students or associated third parties;
- transmitting any other statement which is likely to create any liability (whether criminal or civil and whether for the employee or for the Trust);
- downloading or disseminating material in breach of copyright;
- engaging in online gambling;
- accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.

Where evidence of misuse is found, the Trust may undertake a more detailed investigation in accordance with our Disciplinary Policy, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure.

If necessary, such information may be handed to the police in connection with a criminal investigation.

Digital Cameras

The School encourages the use of digital cameras and video equipment. However, staff should be aware of the following guidelines:

- Photos should only have the pupil's full name if they are on display in a school only. Photos for the website or press must only include the child's first name.
- The use of personal digital cameras in school is not permitted, including those which are integrated into mobile phones, iPads or similar.
- All photos should be downloaded to the Trust network as soon as possible, and thereafter be deleted from the device.

File Storage

Staff members, governors and pupils are provided with their own personal cloud storage area, as well as access to shared cloud storage via the Trust's intranet. Any Trust/ school related work should be stored on one of these cloud drives. Personal files are not permitted in these drives. Staff are responsible for ensuring they have rights for the storage of any file in their area or which they add to shared storage areas for example, copyright music files. Local network storage is being phased out across the Trust, but whilst available, personal and shared network drives are subject to the same principles as cloud storage.

Removable media is being phased out across the Trust. Where still available, it must be stored in accordance with the Information Security Policy, summarised as follows:

- If information/data is to be transferred, it must be saved on an encrypted, password protected, storage device.
- No school data is to be stored on a home computer or un-encrypted storage device.
- No confidential or school data which is subject to the Data Protection Act should be transferred off site unless it is sent by secure email.

Mobile Phones

Mobile phones are permitted in schools with the following restrictions:

- They are not to be used when members of staff are directly supervising or working with children.
- Personal mobile phone cameras are not to be used on school trips. A school may provide digital cameras and/ or trip phones for this purpose.
- All phone contact with parents regarding school issues will be through the Trust's phone system. Personal mobile numbers should not be given to parents or other.

School's will have their own policies and procedures regarding student use of mobile phones.

Use of Whatsapp (or similar messaging apps)

WhatsApp is not permitted for use on Trust-issued devices. Members of staff are able to use WhatsApp on their own devices for personal communication and may wish to utilise these tools for communicating with colleagues outside of working hours. However, staff should not communicate with other staff members for Trust/ School business using their

personal WhatsApp accounts, sharing School related information which could include categories of personal data.

The Trust has a Social Media Policy which should be read in conjunction with this policy. The key requirements for staff are as follows:

- Staff members have a responsibility to protect the reputation of the Trust, staff and students at all times and must treat colleagues, students and associates of the Trust with professionalism and respect whilst using social networking sites.
- Social networking sites should be used responsibly and users should ensure that neither their personal or professional reputation and/or the Trust's reputation, nor the reputation of individuals within the Trust are compromised by inappropriate postings.
- Use of social networking sites for Trust/ school business is not usually permitted, unless via an officially recognised school site and/ or with the permission of the School Business Manager.
- Members of staff will notify the School Business Manager if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the School/setting.
- No school information, communication, documents, videos and/or images should be posted on any personal social networking sites without the permission of School Business Manager.
- No details or opinions relating to any pupil are to be published on any website.
- Users must not knowingly cause annoyance, inconvenience or needless anxiety to others (cyber bullying) via social networking sites.
- No opinions regarding another member of staff, which could cause offence, are to be posted.
- No photos or videos which show pupils of the Trust/ School who are not directly related to the person posting them, should be uploaded to any site other than Trust or School websites, or Trust or School operated social media pages.
- No comment, images or other material may be posted anywhere, by any method that may bring the Trust or the profession into disrepute.
- Users must not give students access to their area on a social networking site (for example, adding a student as a friend on Facebook). If in exceptional

circumstances, users wish to do so, please seek advice from the Trust Safeguarding Lead.

The Trust may exercise its right to monitor the use of its ICT systems. This includes websites accessed, the interception of e-mail and the viewing of data stored, where it believes unauthorised use of the Trust's ICT system is or may be taking place or the system is or may be being used for criminal purposes. Any inappropriate material found will be deleted. Monitoring software is installed to ensure that use of the network is regularly checked by the Trust Safeguarding Lead or school Designated Safeguarding Leads to ensure there are no pastoral or behaviour concerns or issues of a safeguarding or prevent nature.

Other reasons for monitoring the ICT systems include the need to:

- ensure operational effectiveness of the services provided;
- maintain the systems;
- prevent a breach of the law, this policy or any other Trust or school policy;
- investigate a suspected breach of the law, this policy or any other Trust or school policy.

Failure to Comply with Policy

Any failure to comply with the policy may result in disciplinary action. Depending upon the severity of the offence, a breach of this policy may be considered gross misconduct leading to summary dismissal.

Monitoring of the ICT Systems

Any unauthorised use of the Trust's ICT systems, cloud-based ICT systems, the internet, e-mail and/or social networking site accounts which the Trust or school Designated Safeguarding Lead considers may amount to a criminal offence or is unlawful shall, without notice to the user concerned, be reported to the police or other relevant authority.

The Trust reserves the right to audit and/or suspend a user's network, e-mail and/or application account(s) pending an enquiry, without notice to the user concerned.

Appendix 1: acceptable use agreement (staff, Local Academy Committee members, trustees, volunteers and visitors)

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, LOCAL ACADEMY COMMITTEE MEMBERS, TRUSTEES, VOLUNTEERS AND VISITORS	
Name of staff member/Local Academy Committee member/volunteer/trustees/visitor:	
When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), 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 school'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 school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils 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 school	
I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role. I agree that the school will monitor the websites I visit and my use of the school'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 school, and keep all data securely stored in accordance with this policy and the school's data protection policy. I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil 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 school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/Local Academy Committee member/trustee/volunteer/visitor):	**Date:**