



# Pennine Academies Yorkshire

## ICT Acceptable Use & Online Safety Policy

Date Policy Written:	December 2021
Date Policy Ratified:	December 2021
Date Policy to be Reviewed:	December 2022

## **Technology acceptable use agreement for staff**

Whilst Pennine Academies Yorkshire promotes the use of technology, and understands the positive effects it can have on enhancing pupils' learning and community engagement, we must also ensure that staff use technology appropriately. Any misuse of technology will not be taken lightly and will be reported to the headteacher/head of school in order for any necessary further action to be taken. Any equipment loaned is owned by the trust and may be collected in by the Trust ICT Manager for monitoring and maintenance.

This acceptable use agreement is designed to outline staff responsibilities when using technology, whether this is via personal devices or school devices, on or off the school premises, and applies to all staff, volunteers, contractors and visitors.

Whilst it is not possible to cover all eventualities, the following information is published to guide staff on the expectation of Trustees. Any breaches of this policy or operations of the school's equipment outside statutory legal compliance may be grounds for disciplinary action being taken.

This policy document is issued to all staff during their induction where they will be provided with laptops, tablets, mobile phones (where applicable) and passwords giving access to the ICT network and cloud solutions

This policy should be read in conjunction with the school's Child Protection and Safeguarding Policy and the Pennine Code of Conduct policy

### **Policy Coverage**

This policy covers the use by staff of all school or trust owned ICT and communications equipment, examples of which include:

- Laptops, tablets and personal computers;
- ICT network facilities;
- Mobile phones and smartphones;
- Cloud storage & email;
- Image data capture and storage devices including cameras, and video equipment.

This list is not exhaustive.

### **Regulation of Investigatory Powers Act 2000**

Ancillary to their provision of ICT facilities the Trustees assert the employer's right to monitor and inspect the use of staff on any computer (including emails) or telephonic communications systems and will do so where there are grounds for suspecting that such facilities are being, or may have been, misused.

### **Using Technology in School**

- I will only use ICT systems which have been permitted for my use by the headteacher / head of school
- I will electronically lock all devices when not in use
- I will take full responsibility for the equipment and keep it safe.
- I will not allow family or friends to use school equipment.
- I will not leave my device in my car overnight.
- I will only use the approved school / trust accounts that have been provided to me.
- I will not use personal emails to send and receive personal data or information.

- I will not share sensitive personal data with any other staff, pupils or third parties unless explicit consent has been received.
- I will ensure that any personal data is stored in line with the UK GDPR.
- I will delete any chain letters, spam and other emails from unknown sources without opening them and will report any such emails to the Trust ICT Manager
- I will ensure that I obtain permission prior to accessing teaching materials from unapproved sources.
- I will only use the internet for personal use during out-of-school hours, including break and lunch times.
- I will not search for, view, download, upload or transmit any explicit or inappropriate material when using the internet.
- I will not share school-related passwords with pupils, staff or third parties.
- I will report any breaches of password confidentiality to the Trust ICT Manager without delay.
- I will not install any software onto school ICT systems unless instructed to do so by the trust Trust ICT Manager.
- I will ensure any school-owned device is protected by anti-virus software this is monitored by the ICT support contractor if an error is found on my device I will return to school for further inspection
- I will only store data on the Pennine Academies Yorkshire Google Drive
- The use of USB sticks is not permitted.
- I will only store sensitive personal data where it is absolutely necessary and has been encrypted.
- I will give removable media to the trust Trust ICT Manager or ICT Support contractor for safe disposal once I am finished with it.

### **Mobile Devices**

- I will only use school-owned mobile devices for educational purposes.
- I will only use personal mobile devices during out-of-school hours, including break and lunch times.
- I will ensure that personal mobile devices are either switched off or set to silent mode during school hours, and will only make or receive calls in specific areas, e.g. the staffroom.
- I will ensure personal mobile devices are stored in a lockable cupboard located in the staffroom or classroom during lesson times.
- I will not use personal mobile devices to take photographs or videos of pupils or staff.
- I will not use mobile devices to send inappropriate messages, images or recordings.
- I will ensure that personal and school-owned mobile devices do not contain any inappropriate or illegal content.
- I will not use personal or school-owned mobile devices to communicate with pupils.
- I will not use personal or school-owned mobile devices to communicate with pupils or parents
- I will not store any images or videos of pupils, staff or parents on any mobile device unless consent has been sought from the individual(s) in the images or videos.
- In line with the above, I will only process images or videos of pupils, staff or parents for the activities for which consent has been sought.
- I will ensure that I only store school data on my personal device if given permission by the headteacher/HoS I will ensure the device is encrypted and data is pseudonymised

### **Social Media and Online Professionalism**

- If I am representing the school online, e.g. through blogging or on a school social media account, I will express neutral opinions and will not disclose any confidential information regarding the school, or any information that may affect its reputability.
- I will not use any school-owned devices to access personal social networking sites, unless it is beneficial to the material being taught; I will gain permission from the Headteacher/Head of School before accessing the site.
- I will not communicate with pupils or parents over personal social networking sites.

- I will not accept 'friend requests' or 'follow requests' from any pupils or parents over personal social networking sites.
- I will ensure that I apply the necessary privacy settings to any social networking sites.
- I will not publish any comments or posts about the school on any social networking sites which may affect the school's reputability.
- I will not post or upload any defamatory, objectionable, copyright-infringing or private material, including images and videos of pupils, staff or parents, on any online website.
- I will not post or upload any images and videos of pupils, staff or parents on any online website without consent from the individual(s) in the images or videos.
- In line with the above, I will only post images or videos of pupils, staff or parents for the activities for which consent has been sought.
- I will not give my home address, phone number, mobile number, social networking details or email addresses to pupils or parents – any contact with parents will be done through authorised school contact channels.

### **Virtual Communication**

- I will use the school's chosen platform (Google workspace) for Remote Learning Sessions and virtual meetings.
- Where other cloud based systems are required, I will ensure adequate security is in place including the use of passwords and logging out as the call ends.
- Where an external company wishes to use an alternative platform, I will ensure the Trust ICT Manager or ICT support contractor is aware in advance to ensure filtering is in place.
- Where children are invited to a Google Meet, I will only use their unique passcode and will ensure a second adult is present throughout.
- Whilst using Google Meet, I will ensure I am in an appropriate space and remain professional at all times.

### **Working Remotely**

- I will adhere to the principles of the UK GDPR when working remotely
- I will ensure I obtain permission from the Headteacher/Head of School and DPO before any personal data is transferred from a school-owned device to a personal device.
- I will ensure any data transferred from a school-owned device to a personal device is encrypted or pseudonymised.
- I will ensure any sensitive personal data is not transferred to a personal device unless completely necessary – and, when doing so, that it is encrypted.
- I will ensure my personal device has been assessed for security by the trust Trust ICT Manager before it is used for lone working.
- I will ensure no unauthorised persons, such as family members or friends, access any personal devices used for lone-working.
- I will not connect a school / trust owned device to a public wireless network e.g. coffee shop wireless
- I will ensure my personal wireless connection at home is secure before connecting a school device to it

### **Online Resources Guidance**

Do

- Thoroughly check all content before using in class (watch the full video / save the google image as part of your teaching resources)
- Report any content you may come across that could be harmful to your Head

Don't

- Use search engines / websites with content with unregulated content on when in rooms with pupils

- Allow pupils to make web searches that haven't been tested before the lesson
- Assume videos / websites are what the title suggests
- Allow other staff / pupils to use your log on
- Allow other people at home to use school devices

### **Training**

- I will ensure I participate in any online safety training offered to me, and will remain up-to-date with current developments in social media and the internet as a whole.
- I will ensure that I allow the trust Trust ICT Manager and DPO to undertake regular audits to identify any areas of need I may have in relation to training.
- I will ensure I employ methods of good practice and act as a role model for pupils when using the internet and other digital devices.
- I will ensure that I deliver any training to pupils as required.

### **Use of Personal phones and other ICT equipment**

The use of personal phones, tablets & laptop computers is not permitted in any part of the school that pupils use, this includes classrooms, corridors, shared areas and halls. The use of personal devices is not permitted during working hours unless the user is on a break and in a staff only area e.g. staffroom.

Personal equipment is not permitted to be connected to the school or Trusts wireless or wired network connection.

### **Reporting Misuse**

- I will ensure that I adhere to any responsibility I have for monitoring, as outlined in the Pupil E-Safety Policy, e.g. to monitor pupils' internet usage.
- I will ensure that I report any misuse by pupils or staff members breaching the procedures outlined in this agreement to the headteacher/head of school. Members of the central team need to report misuse to the Trust Trust ICT Manager.
- I understand that my use of the device will be monitored by the trust Trust ICT Manager and SLT and recognise the consequences if I breach the terms of this agreement.
- I understand that the headteacher/head of school may decide to take disciplinary action against me, in accordance with the Disciplinary Policy and Procedure, if I breach this agreement.

### **Useful Names and Contacts**

Name	Role	Contact Number	Contact email
Jonathan Duke	Headteacher	07826 523032	j.duke@hps.paymat.org
Jonathan Duke	Designated Safeguarding Lead	07826 523032	j.duke@hps.paymat.org
Kerry Mulroy	Trust ICT Manager	07814 159259	k.mulroy@paymat.org