St Mary's Catholic High School, Leyland

Technology Acceptable Use Agreement

Created: November 2015 Updated: Sept 2022 Review by: Autumn 2024

Statement of Intent

Whilst our school 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 in order for any necessary further action to be taken.

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.
Please read this document carefully, and sign below to show you agree to the terms outlined.

1. Using technology in school

- I will only use ICT systems which have been permitted for my use by the school, such as:
  - Computers.
  - Laptops.
  - Tablets.
- I will only use the approved email 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.

- 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 unless permission has been given for me to do so**, this includes printer and door codes.**
- I will ensure any school-owned device is protected by anti-virus software and that I check this on a weekly basis and inform the Network Manager or IT Technician of any problems.
- The use of removable storage is not allowed and is blocked by the Sophos.
- I will only store sensitive personal data where it is absolutely necessary and has been encrypted.

2. 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 during lesson times.
- I will not use personal mobile devices to take photographs or videos of pupils or staff – I will seek permission from the headteacher/DSL before any school-owned mobile device is used to take images or recordings.
- 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.
- Access the WiFi system using personal mobile devices is permitted by requesting access from the IT Network Manager or IT Technician. I understand school internet access is monitored.
- I will not use personal 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.
- I will not use my personal device in school to watch streaming media services over WiFi, such as Disney+, Netflix, Amazon Video, Hulu and BritBox.

- I will not use my personal device in school to watch pornography or view other inappropriate content.
- 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 any school data stored on personal mobile devices is encrypted and pseudonymised, and give permission for the IT Network Manager to erase and wipe school data off my device remotely if it is lost or as part of exit procedures.

3. 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 mobile devices to access personal social networking sites, unless it is beneficial to the material being taught; I will gain permission from the IT Network Manager 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.

4. Working from home

- I will adhere to the principles of the UK GDPR when working from home.

- I accept remote access is only granted to accounts that have Multi-Factor Authentication (MFA) enabled. As such I consent to the installation of Microsoft's Authenticator App on my phone.
- I will ensure I obtain permission from the 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 and protected by Sophos home.
- 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 IT Network 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 act in accordance with the school's Online Safety Policy when transporting school equipment and data.

5. 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 IT Network 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.

6. Reporting misuse

- I will ensure that I adhere to any responsibility I have for monitoring, as outlined in the Online 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.
- I understand that my use of the internet will be monitored by the IT Network Manager and recognise the consequences if I breach the terms of this agreement.
- I understand that the headteacher may decide to take disciplinary action against me, in accordance with the Disciplinary Policy and Procedure, if I breach this agreement.
- I will alert the Network Manager or IT Technician immediately if I think my account may have been compromised.

THIS PAGE HAS BEEN LEFT BLANK ON PURPOSE

Acknowledgement of Receipt

Please return this to the business manager or complete Electronic Reply

I certify that I have read and understood this agreement, and ensure that I will abide by each principle.

Signed: _____ Date:_____

Print name: _____