



Fulwood and Cadley Primary School



Computing and Technology-acceptable use agreement for staff-2023-24

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

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.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communication technologies for educational, personal and recreational use.
- that school technological systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to technology to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

1. Using technology in school

- I will only use ICT systems which have been permitted for my use by the headteacher, 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 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.
- I will not install any software onto school ICT systems unless instructed to do so by the online safety leader or headteacher.
- I will ensure any school-owned device is protected by anti-virus software and that I check this on a weekly basis.
- I will only use recommended removable media and will keep this securely stored in line with the UK GDPR.
- I will only store data on removable media or other technological devices that have been encrypted or pseudonymised.
- I will only store sensitive personal data where it is absolutely necessary and has been encrypted.
- I will give removable media to the online safety leader for safe disposal once I am finished with it.

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 located in the staffroom or classroom during lesson times and as children are leaving and entering from break.
- I will not use personal mobile devices to take photographs or videos of pupils or staff – I will seek permission from the headteacher 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.
- I will not access the WiFi system using personal mobile devices unless permission has been given by the headteacher or online safety leader.
- 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 any school data stored on personal mobile devices is encrypted and pseudonymised, and give permission for the online safety leader to erase and wipe data off my device if it is lost or as part of exit procedures.
- I will ensure my Smart Watch has Bluetooth turned off and notifications disabled during lesson time.
- I will ensure the safety checks for iPad lock ups are adhered to and signed daily.
- I will ensure the keys for the iPad lock ups are left in the Server Room at the end of every day

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 headteacher 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 will ensure I obtain permission from the headteacher 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 DPO and online safety leader 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 online safety leader 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 online safety leader 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 understand that I must use school technological systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the computing systems and other users. I recognise the value of the use of technology for enhancing learning and will ensure that pupils receive opportunities to gain from the use of technology. I will, where possible, educate the young people in my care in the safe use of technology and embed e-safety in my work with young people.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name

Signed

Date