



Acceptable Use Policy for Staff and Volunteers

Last Review:	June 2020
Committee:	SLT
Date Ratified:	04/06/2020
Next Review:	June 2022

1. Purpose

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.

- 1.1. All users should have an entitlement to safe access to the internet and digital technologies at all times. 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 communications technologies for educational, personal and recreational use.
 - School systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
 - Staff are protected from potential risk in their use of technology in their everyday work.
- 1.2. The school will try to ensure that staff and volunteers have good access to digital technology to enhance their work, to enhance learning opportunities for students' learning and will, in return, expect staff and volunteers to agree to be responsible users.
- 1.3. This policy has been informed by a range of material from organisations with experience and expertise in the area of online safety. These include the South-west Grid for Learning (SWGfL) and the Child Exploitation and Online Protection Centre (CEOP).
- 1.4. This policy should be read in conjunction with the School's Safeguarding and Child Protection, Data, Online Safety and Behaviour policies.

2. Staff/Volunteer Acceptable Use Policy Agreement

- 2.1. I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.
- 2.2. For my professional and personal safety:
 - I understand that the school will monitor my use of the school digital technology and communications systems.

- I understand that the rules set out in this agreement also apply to the use of these technologies (e.g. laptops, email, etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of to the appropriate person.

2.3. I will be professional in my communications and actions when using school IT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital/video images.
- I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name or other personal information those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with students and parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

2.4. When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).
- I understand that I am responsible for my actions in and out of the school.
- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.

2.5. I understand that if I fail to comply with this Acceptable Use Policy Agreement I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors/Directors and/or the Local Authority and in the event of illegal activities, the involvement of the police.

2.6. Expectations regarding safe and responsible use of social media will apply to all staff and volunteers and exist in order to safeguard both the school and the wider community, on and offline. Examples of social media may include:

- blogs, wikis
- social networking sites, forums, bulletin boards
- multiplayer online gaming, apps
- video/photo sharing sites
- chatrooms, instant messenger

2.7. Expectations regarding the use of the school email system and the school's learning platforms e.g. Show My Homework and live streaming / video conferencing platforms including Microsoft Teams and Zoom will apply to all staff/volunteers to safeguard both yourself and the school on and offline:

- When using Show My Homework, live streaming and video conferencing platforms I will ensure that I do not violate copyright laws by reproducing work that is protected by a copyright. This includes copyrighted multimedia content such as music and video clips accessed through unapproved sites.
- Show My Homework is run through Internet domains purchased and owned by Oldfield School. It is only to be used for educational use with students and staff.
- I will ensure that when live video and audio is being used, there has been careful consideration of the location that everyone uses. It is possible that students may be in their bedrooms and this may not be appropriate. If a location is unsuitable I will ask the student to leave the meeting and move to a different location.
- At the beginning of a live streaming/video session I will be clear about the expectations of student behaviour (e.g. a 'classroom standard' of behaviour is expected from all participants).
- I will consider my privacy settings before posting – (e.g. YouTube has a variety of settings (Public, Unlisted, Private, Comments Allowed/Not Allowed) that will determine who can see and comment on the video.
- I will make a note of the conference timing and who participated, including those that arrived/departed early or late. I will be clear about whether it is acceptable for students to record events and expectations/restrictions about onward sharing.
- I will report immediately to the Designated Safeguarding Lead any safeguarding incidents or potential concerns according to our Safeguarding and Child Protection Policy.
- In no circumstances when using either the school email system or school learning platforms should personal information including full names, addresses, birth dates, phone numbers or other personal identifiers be sent within the context of the message or the work.
- Show My Homework and live streaming/video conferencing platforms are to be used between students and staff to facilitate collaboration, planning, and research for school-related assignments/work only and not for personal contact.
- Show my Homework and the school email system are to be used to communicate with a student regarding assignments, class projects, and class work and not for personal correspondence regarding non-related school information.

2.8. The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (laptops, tablets, mobile phones, USB devices, etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails unless the source is known and trusted or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes).
- I will agree to the School's Acceptable Use declaration (see Appendix 1 – Staff ICT compliance) when I log onto the school network.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others.

2.9. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.

- I will not install or attempt to install programmes of any type on a machine or store programmes on a computer nor will I try to alter computer settings unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others as outlined in the School Data Policy. Where digital personal data is transferred outside the secure local network it must be encrypted. Paper based protected and restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student data to which I have access will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

Name: Signature: Date:

Appendix 1 : Staff ICT Compliance

I will take care when opening emails, and that I will not assume that email is a trusted means of communication, including:

- Not opening links or attachments which I am not expecting – instead I will verify the validity of the email by other trusted means (e.g. phone call, SMS).

I will take care when sending emails by taking measures to ensure the email address is accurate.

I will take measures to secure personal data within external emails by:

- Encrypting the contents within a file or folder (password protected), ensuring the password is shared using a different communication method (e.g. phone call, SMS).
- Using anonymisation or pseudonymisation (using a unique identifier which only the sender/recipient can match up to a name).

I will ensure **clear desk / clear screen** principles are maintained, by:

- Clearing away documents containing any personal or special data when I am away from my desk for a short period.
- Locking away personal data when I am away from my desk for an extended period (e.g. packing up for the day).
- Locking my screen when I am away from my device using \square + L

I will ensure personal data is not removed from the school site by:

- Only storing electronic personal data (e.g. electronic markbooks, assessment data with student names) on the school server, and not saving this in any removable device (such as a memory stick).
- Only accessing data securely at home through remote access, not using public networks or computers. Ensuring that remote access connection is terminated immediately after use.