Pewsey Vale School

Headteacher: Carol Grant

ICT Acceptable Use Policy and E-Safety Guidance for Staff and Students (P46)

Responsibility: Carol Grant - Headteacher

Next Review: May 2018

• Reviewed by CG	May 2017
• Implemented by P&S Committee	12 May 2017
• Verified by FGB	25 May 2017

P&S Approving signature: ___________________________ Date: ________

Head Teacher signature ____________________________Date: ________

Chair of Governors signature ____________________________Date: ________

Historical Reviews/Update:

- introduced September 2015
- Reviewed June 2016

Acceptable Use Policy for Staff

Social networks: Members of staff should never knowingly become “friends” with students or ex-students under the age of 18 on any social networking site or engage with children on internet chat.

Email Communication: All members of staff should use their school email address for conducting professional business. This includes communicating with colleagues, parents and students. When emailing parents always use formal language and copy in your line manager. When emailing colleagues ensure that you restrict the recipients to only those who need to read the email you are sending out. Use of ‘all staff’ email should be mainly for the purposes of SLT and the main office to support the strategic aims and day to day running of the school, except in emergencies. As far as possible emails should be restricted to working hours so as not to burden colleagues with additional workload.

Remote Access: Staff are permitted to access their school documents using the secure remote desktop protocol (RDP). Please ensure full compliance with data protection and do not leave your home computer unattended when logged in.

Passwords: Keep your passwords private. Passwords are confidential and individualised to each person. On no account should a member of staff allow a student to use a staff login.

Data Protection: Where a member of staff has to take home sensitive or confidential information, sufficient safeguards should be in place to prevent loss or misuse, i.e. is it really necessary to take it all home, can it be encrypted and does it have to be on a USB memory stick that can be easily misplaced? All data relating to staff, students and parents must be kept private and confidential.

Personal Use: Staff are not permitted to use ICT equipment for personal use without SLT approval. If personal use is permitted the boundaries and expectations of use within school should be adhered to.

Images and Videos: No images or videos should ever be uploaded to a website or social network without the express permission of parents or the child’s carer. Similarly no personal information (name, date/place of birth, mobile number, email address etc.) should ever be shared.

Use of Personal ICT devices/Bring Your Own Devices (BYOD): Use of personal ICT equipment (i.e. mobile phones, cameras, personal laptop etc.) is at the discretion of the Senior Leadership Team. Any such use should be stringently checked for up to date anti-virus and malware checkers. Use of personal ICT devices is subject to the same Acceptable Use Policy. Pictures or videos of children must never be taken using personal ICT devices.

Internet access: You must not access, or attempt to access, websites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. It is recognised that under certain circumstances inadvertent access may happen. Should you or a student access any of these sites unintentionally you should report the matter to a member of the Senior Leadership Team so that it can be logged.

Inappropriate/Illegal content: Access to any of the following should be reported to the Police: images of child sexual abuse (sometimes incorrectly referred to as child pornography). These are images of children apparently under 16 years old involved in sexual activity or posed to be sexually provocative; adult material that potentially breaches the Obscene Publications Act; criminally racist material in the UK.

Reporting concerns: It is the duty of staff to support the school’s safeguarding policy and report any behaviour (staff or students), which is inappropriate or a cause for concern, to a member of the Senior Leadership Team.

Monitoring: Emails and internet activity are subject to monitoring.

ICT Acceptable Use Policy for Students

Advice and Guidance

Use of the Internet - the internet is not to be used to access anything which is illegal, or anything that someone else may find offensive. This would include indecent images, discrimination, racial or religious hatred. If you are unsure, or if you come across anything which makes you feel uncomfortable, you should turn your computer monitor off and let a teacher know.

Logins and Passwords - every person has a different computer login and password. You should never allow anyone else to use your details. Change your password if you think someone else may have your details.

Social Networking - never upload pictures or videos of others without their permission. It is not advisable to upload pictures or videos of yourself as they can easily be manipulated and used against you. You should never make negative remarks about the school/organisation or anyone within the school/organisation. Always keep your personal information private and never post personal information such as your full name, date of birth, address, school, phone number etc. Consider using a nickname and only inviting people you know. Universities and future employers have been known to search social networking sites. Beware of fake profiles and people pretending to be somebody else. If something doesn't feel right follow your instincts and report it to an appropriate adult. Never create a false profile as a joke and pretend to be somebody else. This can have serious consequences.

Chat Rooms - some social networking sites have a chat facility. You should never chat to anyone that you don't know or don't recognize. It is recommended that you never meet a stranger after meeting them online. If you do, always inform your parents and take one of them with you.

Security - you should never try to bypass any of the security in place, this includes using proxy bypass sites. This security is in place to protect you from illegal sites, and to prevent hacking into other people's accounts.

Copyright - you should never take information from the internet and use it as your own. A lot of information is copyright, which means that somebody else owns it and it is illegal to use this information without permission from the owner. If you are unsure, ask an adult.

Mobile Phones - Most mobile phones offer the same services as a computer, i.e. Facebook, YouTube, email access etc. This can be a great way of keeping in touch with your friends and family. But, in the same way that some internet services can be used inappropriately, the same is true with mobile phones. Never take inappropriate pictures of yourself and send to your friends or upload onto social networking sites. Never forward inappropriate pictures that you have received from somebody else as this could be illegal.

Cyber-bullying – Never use the internet or other ICT communication to bully or make fun of people. It can have very serious consequences. Report incidents of cyber-bullying to a member of staff and/or a parent/carer.

ICT equipment - treat all school equipment with care and respect. Report any problems to a member of staff. Sanctions – failure to follow this guidance, or deliberate misuse of school ICT, may result in a sanction.