Acceptable Use Policy - Staff

Co-ordinator	**School Business Manager**
Date of Completion	**January 2023**
Date of adoption by Governors	**April 2023**
Date to be reviewed	**January 2024**

Overview
Technology is now entwined in our modern lives with everyday use of social media and web-based communication a standard practice. It is therefore important to ensure good awareness both of the possibilities to learn, create and share ideas and also the risks that these freedoms bring both to the welfare of staff and students and to the integrity of the IT systems that the school relies on to provide learning and teaching.

All users who access our school systems are entitled to safe access to the internet and IT systems at all times. This policy is intended to provide a working framework for staff to uphold the positive ideals of the technology we use while providing a safe learning environment and protecting the data we manage in the course of our services to students and their families.

The policy will outline how:

- Staff must ensure they are responsible users of the IT systems provided and that they make sound judgements while using the Internet and other communications technologies for educational and personal use.
- The school IT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- Staff can ensure they are protected from potential risk in their use of technology for educational and personal use.

Schools AUP Agreement:

I agree that I must use school IT systems in a responsible way. I must do so to ensure there is no risk either to my own safety or to the safety and security of the students and school IT systems. I will, where possible, guide students in the safe use of technology with a strong focus on safe and responsible use of the internet and online services.

For the purposes of safeguarding and security:

- I understand that the school/council reserves the right to monitor, access and review my use of the Internet without the additional consent being required. Surveillance may be undertaken for the purposes of audit, security or where there is reason to believe that a breach of this policy has occurred.
- I understand the rules in this document apply equally to the use of school and personal devices and systems (e.g. laptops, email, VLE etc.) outside of school
- I understand the importance of appropriate controls on the transfer and sharing of personal data (digital or paper-based) out of school.
- I understand that the school IT systems are primarily intended for educational use.
- I will only use the systems for personal or recreational use when appropriate.

- I will only use the school/council's electronic mail systems for school use and not for anything private unless agreed.
- I will never disclose my username or password to anyone else, nor use any other person's username and password to access systems not provided to me.
- I understand that I should not record any password where it is possible that someone may view it or steal it.

  I will immediately report any incident or activity I am aware of which may be illegal, inappropriate or present risk to the school or individuals to my Line Manager or the Executive Head Teacher. Where the concern or issue persists and cannot be resolved the Executive Head Teacher may escalate the matter to the Chair of Governors.

I will use all the school IT and communication systems professionally. In doing so:

- I will not access, copy, alter, share or delete any other user's files, without their express permission.
- I will communicate with others in a professional manner and refrain from any use of aggressive or inappropriate language.
- I will ensure that, if I wish to take or publish images of others I will check that appropriate consent is recorded by the school in lines with the school's Safeguarding Policy.
- I will only use school provided and managed equipment to record these images unless I have explicit permission to do otherwise.
- I will ensure that any published photos do not identify individuals by name or show other personal information and that photos and images are only used on a school approved and controlled platform.
- I will only use social networking services in school in accordance with the school's policies.
- All communication will be professional in tone and manner.
- I will ensure that I do not share my personal contact information and only ever use contact details provided by the school.
- I will not engage in any online activity that may compromise my professional integrity or provide a risk to the students, my colleagues, the school IT systems or myself.

The school and the local authority will provide safe and secure access to school IT systems and services and maintain the availability and integrity of the school systems in support of learning and teaching. However, any use of personal mobile devices (such as but not limited to, laptops/tablets/ mobile phones) in school, must be in accordance with rules set out in this agreement, as per any school managed equipment.

Staff members must:

- Ensure that any such personal devices are protected by up to date security patches and anti-virus software and are free from viruses.
- Remain vigilant when accessing emails. Never click on any hyperlinks in emails or any attachments to emails, unless the sender is known and trusted.
- Report any concerns about emails or communication received on any other school or personal IT system must be flagged to Line Manager or the Executive Head Teacher.
- Ensure all professional work is stored in the appropriate, provided, location on the school network or systems to guarantee appropriate levels of backup and malware scanning.
- 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.
- Not try to use any applications, such as VPN, that might allow them to bypass the filtering/security systems in place to provide a safe learning and teaching environment.
- Staff should not install any applications on school devices without consultation and support from Line Manager. Neither should they change settings put in place by the school to ensure appropriately managed devices.
- Report any damage to or faults in school equipment onto the Schools ICT job list
- Only share personal information collected and managed by the school with others as their role permits or when required by law or by school policy to disclose such information to an appropriate authority. Any data sharing must be by approved and encrypted communication services provide by the school or their business partners. (Local Authority)
- Ensure that copyrighted resources are only used or shared with appropriate permissions. Copyrighted work will not be downloaded or shared including music and videos unless an exemption applies for teaching purposes.
  These purposes include:
    - the copying of works in any medium as long as the use is solely to illustrate a point, it is not done for commercial purposes, it is accompanied by a sufficient acknowledgement, and the use is fair dealing. This means minor uses, such as displaying a few lines of poetry on an interactive whiteboard, are permitted, but uses which would undermine sales of teaching materials are not;
    - performing, playing or showing copyright works in a school, university or another educational establishment for educational purposes. However, it only applies if the audience is limited to teachers, pupils and others directly connected with the activities of the establishment. It will not generally apply if parents are in the audience. Examples of this are showing a video for English or drama lessons and the teaching of music. It

is unlikely to include the playing of a video during a wet playtime purely to amuse the children;
- by recording a TV programme or radio broadcast for non-commercial educational purposes in an educational establishment, provided there is no licensing scheme in place. Generally, a licence will be required from the Educational Recording Agency;
- making copies by using a photocopier, or similar device on behalf of an educational establishment for the purpose of non-commercial instruction provided that there is no licensing scheme in place. Generally, a licence will be required from the Copyright Licensing Agency.

These and other, exemptions to copyright are listed here:
https://www.gov.uk/guidance/exceptions-to-copyright

Exemptions

Certain staff working for the school or council ICT teams may be exempted from some areas of this policy in order for them to carry out their normal duties. This only applies to staff who have been nominated as exempt by the Executive Head Teacher with the details of their exemption specified.

Data Protection

The school/council both have nominated Data Protection Officers who are tasked with ensuring that the school/council records, stores and transmits data in compliance with the Data Protection Act 1998.

The Data Protection Act 1998 puts certain legal obligations on the school/council for the recording and storing of personal information. Any queries should be addressed to the Data Protection Officer.

Employees responsible for computer systems that record personal information must ensure that all such systems comply with the Data Protection Act 1998.

Any employee who develops a database, spreadsheet or other computer system that records personal information must ensure that the system complies with the Data Protection Act 1998.

Staff Changes

Line managers, or other nominated officers, should inform the Executive Head Teacher of all new employees so that the appropriate usernames and passwords can be created.

When an employee leaves their job, whether leaving the school/Council or not, the line manager, or other nominated officer, must inform the Executive Head Teacher immediately so that all usernames and passwords for that employee can be suspended as appropriate.

Encryption

Files may be password protected where the application software has such a facility built in. Where files are password protected employees must make provision for line managers and/or colleagues to gain access to the file in their absence. Employees must not install or use any other encryption software without the written permission of the Executive Head Teacher or one of the nominated officers.

Email - Good Practice Guidelines

The following good practice guidelines should be observed:

- e mail is intended for business use and whilst correspondence is generally briefer than other correspondence, try to use correct grammar and spelling making use of the spell checking facilities on the e mail system;
- consider the correspondence to be permanent and do not assume that the e mail, when deleted, will be lost forever;
- take care when communicating sensitive information;
- take care when communicating with someone in another country as insensitive use could lead to litigation in that country;
- if training is required on the use of the council's e mail system then discuss your requirements with your line manager;
- keep a permanent record of an e mail containing substantive advice;
- do not communicate information via e mail that you would not be prepared to say to the recipient if you were talking face to face;
- avoid using upper case in e mail as it is generally interpreted as shouting;
- wherever possible, other people's comments or observations should be communicated verbatim by using the "threading" capability of e mail i.e. using Reply and Forward options so that the message history is retained (do not quote comments or observations from other people as a quote may be taken out of context);
- care should be taken to address electronic mail to the intended recipient as misaddressing is common;
- clearly title messages so that the contents can be understood before the message is opened;
- clearly mark a message "for information" if no action is required;
- make it clear what action or response is required from each recipient;
- do not copy or forward unnecessary messages to others;
- approval of the Executive Head Teacher should be sought prior to searching any web-sites which would normally be deemed inappropriate.

Ownership and Privacy

All programs stored on a school/council owned computer are the property of the school/council and not individual employees.

An employee may be granted access to use a workstation at the discretion of management and the school/council reserves the right, in its sole discretion, to suspend or terminate any persons use of any or all workstations, at any time. In addition the school may take disciplinary action against any person who misuses workstations or systems accessible through it.

The school/council reserves the right to monitor, access and review an individual's use of workstations without the additional consent being required from any employee. Surveillance may be undertaken for the purposes of audit, security or where there is reason to believe that a breach of this policy has occurred.

Every workstation has a designated person responsible for its use, for the software resident in the machine and for compliance of this policy. This person will be one of the following:

- the occupant of the desk on which the machine resides;
- the manager of an area where workstations are a shared resource for a group of users;
- a user allocated a portable workstation on a temporary or permanent basis.

Executive Head Teacher/line managers must retrieve hardware, software and equipment from employees, contractors and temporary staff leaving their employment

Offsite Use

The following procedures apply where an individual requests the use of ICT hardware off site:

- the individual must seek authorisation from their line manager stating the nature and duration of use;
- the employee and their line manager must sign a document stating the item of equipment, serial number or other relevant identification, the date that the equipment was taken from the school/council's premises and the duration that it will be off site;
- the employee and their line manager must sign a document stating the date that an item of equipment is returned to the school/council's premises;
- the employee accepts responsibility for the equipment once it has been signed for;
- the Executive Head Teacher /ICT team must be informed on the first occasion that an item of hardware is used off site and the documents referred to above must be made available for their inspection as required;

Software

The software installed onto workstations is very tightly controlled and this may be done by the use of automatic control software installed on the workstation. The following restrictions apply to all software:

- all software installed must be properly licensed; the use of all software must comply with the conditions of the relevant licence agreement;
- all software installed must be relevant to the work of the operator of that workstation or the team or department in which it is based;
- any installation of software must only be done with the permission of the Executive Head Teacher /council Head of ICT (or nominated representative);
- free, public domain or shareware software is subject to the same restrictions on use as all other software and must only be installed in compliance with this policy;

- employees must not attempt to circumvent any security system installed on a workstation by management, this includes, but is not limited to, remote control software, automatic control software, lockdown software and antivirus software.

Telephones

The telephones are designed for business use only. Personal use is only permitted in the following circumstances:

- authorisation has been sought from the employee's line manager, and the call is urgent and could not wait until an appropriate work break;
- the call is connected with the employee having to work later than expected;
- the call is a very brief internal call;

Employees must not use the school's telephone system or their own personal mobile phones to receive private calls whilst working unless the call is urgent.

The school/council reserves the right, in its sole discretion, to suspend or terminate any persons use of any telephone. In addition the school may take disciplinary action against any person who misuses the telephone system.

Telephone lines must not be connected, to any equipment, without the permission of the Executive Head Teacher or one of the nominated officers.

I have read and understood the above and agree that:

- I am responsible for upholding the requirements laid out above at all times and that even while in personal time I am representing the values and integrity of the school.
- This Acceptable Use Policy applies not only to my work and use of school-provided IT equipment but also applies to my use of school IT systems on personal equipment both at school and on other private or public networks.
- If I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action as per the terms laid out in the school's Disciplinary Procedure.

Name:	
Signed:	
Date:	