1. Guidelines for Staff and Governors

The school has provided computers for use by staff as an important tool for teaching, learning, and administration of the school. Use of school computers and laptops, by members of staff is governed at all times by the following policy. Please ensure you understand your responsibilities under this policy, and direct any questions or concerns to the IT Network Manager in the first instance.

All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. Deliberate abuse of the school's computer system may result in disciplinary action and civil and/or criminal liability.

The school recognises that the distinction between computer use at work and at home is increasingly blurred, with many of us now using our own computers for work. Staff should consider that this policy applies whenever you are undertaking an activity that stems from your employment with the school.

2. Computer Security and Data Protection

a) You will be provided with a personal account for accessing the computer system, with your own username and password. This account will be tailored to the level of access you require, and is for your use only. As such, **you must not disclose your password to anyone**, including IT support staff. You will be prompted to change your password every 180 days.
b) You **must not allow a pupil to have individual use of a staff account** under any circumstances, for any length of time, even if supervised.
c) When leaving a computer unattended, you **must** ensure you have either logged off your account, or locked the computer (eg. by pressing the WINDOWS key + L) to prevent anyone using your account in your absence.
d) You **must not** store any sensitive or personal information about staff or students on any device (such as a USB memory stick, portable hard disk, personal computer etc.) unless that storage system is encrypted and approved for such use by the school.
e) You must not publish material about a pupil where parents have requested the school not to do so.
   To ensure data is safely backed up, it must be stored centrally on the school network. This is the safest place to store data to minimize the risk of accidental loss of information.
f) You **must** ensure that items of portable computer equipment (such as laptops, digital cameras, or portable projectors) are securely stored in a locked room or cupboard when left unattended.
g) Equipment taken offsite is not insured by the school. If you take any school computer equipment offsite, you should ensure that adequate insurance cover has been arranged to cover against loss, damage, or theft.
h) School-related sensitive and confidential material should only be printed to the FindMe queues or to printers located in staff offices or the staffroom.

3. Personal Use

The school recognises that occasional personal use of the school's computers is beneficial both to the development of your IT skills and for maintaining a positive work-life balance. Such use is permitted, with the conditions that such use

a) **must** comply with all other conditions of this AUP as they apply to non-personal use, and all other school policies regarding staff conduct;
b) **must not** interfere in any way with your other duties or those of any other member of staff;
c) **must not** have any undue effect on the performance of the computer system; and
d) **must not** be for any commercial purpose or gain unless explicitly authorized by the school.

Personal use is permitted at the discretion of the school and can be limited or revoked at any time.

4. Use of your own Equipment

a) Any mains-operated personal computer or electrical equipment brought on site, for any use, is subject to a Portable Appliance Test (PAT) by site maintenance staff, and **must not** be used until approved. This test must be performed at regular intervals as required by school's normal rules on electrical safety testing.
b) You **must not** connect personal computer equipment to school networked computers without prior approval from IT Network staff, with the exception of storage devices such as USB memory sticks and personal digital cameras.
c) If you keep files on a personal storage device (such as a USB memory stick), you **must** ensure that other computers you connect this storage device to (such as your own computers at home) have an up-to-date anti-virus system running to protect against the proliferation of harmful software onto the school computer system.

5. Conduct

a) You **must** at all times ensure your computer usage is professional, ethical and lawful, which includes being polite and using the system in a safe, legal and business appropriate manner. Among uses that are considered unacceptable are the following:
    - Using, transmitting, or seeking inappropriate, offensive, pornographic, vulgar, suggestive, obscene, abusive, harassing, threatening, racist, sexist, or defamatory language or materials;
    - Making ethnic, sexual-preference, or gender-related slurs or jokes.
    - *(This list is not exhaustive)*
b) You **must** respect, and not attempt to bypass, security or access restrictions in place on the computer system.

c) You **must** not intentionally damage, disable, or otherwise harm the operation of computers.
d) You **must** make efforts not to intentionally waste resources. Examples of resource wastage include:
    - Excessive downloading of material from the Internet;
    - Excessive storage of unnecessary files on the network storage areas;
    - Use of computer printers to produce class sets of materials, instead of using photocopiers.
e) You should avoid eating or drinking around computer equipment.

6. Use of Social Networking websites and online forums

Staff must take care when using social networking websites and apps such as Facebook, Twitter, Instagram, Snapchat , even when such use occurs in their own time using their own computer. Social Networking sites invite users to participate in informal ways that can leave you open to abuse, and often make little or no distinction between adult users and children.

a) You **must not** add a pupil to your 'friends list'.
b) You **must** ensure that personal information is not accessible via a 'Public' setting, but ensure it is set to a 'Friends only' level of visibility.
c) You should avoid contacting any pupil privately via a social networking website, even for school-related purposes.
d) You should take steps to ensure that any person contacting you via a social networking website is who they claim to be, and not an imposter, before allowing them access to your personal information.
e) Staff should also take care when posting to any public website (including online discussion forums or blogs) that their comments do not harm their professional standing or the reputation of the school – even if their online activities are entirely unrelated to the school.
f) Misuse of online activities, in school or outside of school, can lead to disciplinary action being taken by the school.
g) Unless authorised to do so, you **must not** post content on websites that may appear as if you are speaking for the school.
h) You should not post any material online that can be clearly linked to the school that may damage the school's reputation.
i) You should avoid posting any material clearly identifying yourself, another member of staff, or a pupil, that could potentially be used to embarrass, harass, or defame the subject.

7. Use of Email

All members of staff with a computer account are provided with an email address for communication both internally and with other email users outside the school. The following considerations must be made when communicating by email:

a) E-mail has the same permanence and legal status as written hardcopy (paper) documents and may be subject to disclosure obligations in exactly the same way. Copies of e-mails may therefore have to be made available to third parties. You **must** be cautious when sending both internal and external mails. The professional standards that apply to internal memos and external letters must be observed for all e-mail.
b) E-mail to outside organisations has the same power to create a binding contract as hardcopy documents. Check e-mail as carefully as written contracts, always use a spell checker and, where appropriate, obtain legal advice before sending. You **must not** purchase goods or services on behalf of the school via e-mail without proper authorisation.
c) All school e-mail you send should have a signature containing your name, job title and the name of the school.
d) E-mail is not a secure method of communication, and can be easily copied, forwarded and archived. Unless explicitly authorised to do so, you **must not** send, transmit, or otherwise distribute proprietary information, copyrighted material, trade secrets, personal data or other confidential information belonging to the school.
e) Having an external e-mail address may lead to receipt of unsolicited e-mail containing offensive and/or sexually explicit content. The school will take measures to minimise the receipt and impact of such content, but cannot be held responsible for material viewed or received by users from the Internet.
f) You must not send chain letters or unsolicited commercial e-mail (also known as SPAM).

8. Supervision of Pupil Use

a) When arranging use of computer facilities for pupils, you must ensure supervision is available.
b) Supervising staff are responsible for ensuring that the Acceptable Use Policy for pupils is enforced.

9. Privacy

a) Use of the school computer system, including your email account and storage areas provided for your use, may be subject to monitoring by the school to ensure compliance with this Acceptable Use Policy and applicable laws. This may include remote monitoring of an interactive logon session. In particular, the school does keep a complete record of sites visited on the Internet by both pupils and staff, however, usernames and passwords used on those sites are NOT monitored or recorded.
b) You should avoid storing non-school related data on the school computer system that is unrelated to school activities (such as personal passwords, photographs, financial information etc.).

c) The school may also use measures to audit use of computer systems for performance and diagnostic purposes.
d) **Use of the school computer system indicates your consent to the above described monitoring taking place.**

10. Confidentiality and Copyright

a) Respect the work and ownership rights of people outside the school, as well as other staff or pupils.
b) You are responsible for complying with copyright law and licenses that may apply to software, files, graphics, documents, music, messages, and other material you wish to use, download or copy. Even if materials on the school computer system or the Internet are not marked with the copyright symbol (©), you should assume that they are protected under copyright laws unless there is an explicit permission on the materials to use them.
c) You **must** consult a member of IT Network staff before placing any order of computer hardware or software, or obtaining and using any software you believe to be free. This is to check that the intended use by the school is permitted under copyright law (as well as to check compatibility and discuss any other implications that the purchase may have). Do not rely on the claims of suppliers, who do not have specific knowledge of the school's systems.

11. Reporting Problems with the Computer System

It is the job of the IT Network Manager to ensure that the school computer system is working optimally at all times and that any faults are rectified as soon as possible. To this end:

a) You should report any problems that need attention to a member of IT support staff as soon as is possible. Problems that seriously hinder your job or teaching and require immediate attention should be reported by telephone; any other problem **must** be reported via email.
b) If you suspect your computer has been affected by a virus or other malware, you **must** report this to a member of IT Network staff **immediately**.

Reporting Breaches of this Policy

All members of staff have a duty to ensure this Acceptable Use Policy is followed. You **must** immediately inform a member of the IT Network staff, or the Headteacher, of abuse of any part of the computer system. In particular, you should report:

c) any websites accessible from within school that you feel are unsuitable for staff or student consumption;
d) any inappropriate content suspected to be stored on the computer system. This may be contained in email, documents, pictures, etc;
e) any breaches, or attempted breaches, of computer security; or

f) any instance of bullying or harassment suffered by you, another member of staff, or a pupil via the school computer system.

Reports should be made to a senior member of staff. All reports will be treated confidentially.

12. Review and Evaluation

This policy will be reviewed regularly and in response to any changes affecting the basis of the original risk assessment, for example: significant security incidents, new vulnerabilities and significant changes to the organisation or technical infrastructure. Changes to this policy will be communicated to all staff.

13. Notes

"Sensitive personal information" is defined as information about an individual that is protected by law. An exact definition can be found in GDPR/DPA 2018 under the title of "special category data". Examples of such data include addresses and contact details of individuals, dates of birth, and pupil SEN data. This list is not exhaustive.

When this policy was reviewed, an equality impact assessment was conducted to ensure any changes did not have an adverse effect under the terms of the Equality Act 2010. Should you have any comments regarding this policy, please contact the school.