Computing Acceptable Use Policy for Staff

Computer Security and Data Protection

- You will be provided with a personal account for accessing the school network, with your own username and password - you must not disclose your password to anyone.
- You must not allow a pupil to have use of your staff account under any circumstances.
- When leaving a computer unattended, you must ensure you have either logged off your account or locked the computer.
- You must not store any sensitive or personal information about staff or students on any portable storage system unless that storage system is encrypted and approved for such use by the school.
- You must not transmit any sensitive or personal information about staff or students via email without the data being encrypted by a method approved by the school.
- You must ensure that items of portable computer equipment are securely stored when left unattended.

Personal Use

Occasional personal use of the school's computers is permitted, with the conditions that such use

- must comply with this acceptable use policy and all other school policies regarding staff conduct;
- must not be for any commercial purpose or gain.

Use of your own Equipment

- You **must not** connect personal computer equipment to school computer equipment without prior approval, with the exception of storage devices such as USB memory sticks.
- 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.

Conduct

You **must** at all times conduct your computer usage professionally. 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;
- Attempting to bypass security or access restrictions in place on the computer system.
- Intentionally damaging, disabling, or otherwise harming the operation of computers.

Use of Social Networking websites and online forums

Staff must take care when using social networking websites, even when such use occurs in their own time using their own computer.

In particular, staff must not add a pupil to their 'friends' or contact them via a social networking site.

Staff should take care when posting to any public website 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.

- Unless authorised to do so, you **must not** post content on websites that may appear as if you are speaking for the school.
- You should not post any material online that may damage the school's reputation, or be used to embarrass, harass, or defame the school or its staff.

Use of email

All members of staff with a computer account are provided with an email address. The following considerations must be made when communicating by email:

- Copies of e-mails may have to be made available to third parties.
- All school e-mail you send should be sent from your school e mail account.
- Unless explicitly authorised to do so, you **must not** send, transmit, or otherwise distribute proprietary information, copyrighted material or other confidential information belonging to the school.

Engaging with pupils online

When delivering a lesson online, reading a story or otherwise recording for broadcast to children, staff should –

- Record against a neutral background
- Dress like they would for school
- Ensure no other tabs are visible on their screen
- Use professional language

Privacy

- Use of the school computer system is subject to monitoring by the school. In particular, the school keeps a complete record of internet sites visited by both pupils and staff.
- You should avoid storing sensitive personal information on the school computer system.

Reporting problems with the computer system

You should report any problems that need attention to a member of IT support staff as soon as is feasible. 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

You must immediately inform the Headteacher of abuse of any part of the computer system. In particular, you should report:

- any websites accessible from within school that you feel are unsuitable
- any inappropriate content suspected to be stored on the computer system.
- any breaches, or attempted breaches, of computer security; or
- any instance of bullying or harassment suffered by you, another member of staff, or a pupil via the school computer system.

All reports will be treated confidentially.