Acceptable Usage Policy Staff

Linked to 360Safe AUP Guidelines

This document has been written to ensure that staff use technology throughout the school appropriately. If they have any questions regarding this policy, they should direct them to Senior Management Team or the Computing Coordinator.

Staff are expected to:

- Use computers and equipment with care and ensure children do the same e.g. water bottles should stay away from machines
- Ensure that they have a sensible password
- Ensure that usernames and passwords are not shared with children or other staff
- Ensure that they log off when they have finished using a computer
- Make use of resources such as cameras and microphones but ensure that these are returned after their use. They should also endeavour to remove pictures/files on return too
- Try not to be wasteful, in particular when it comes to batteries, printer ink and paper
- Ensure that online dialogue (e.g. blog posts or emails) with other schools, parents or children remains professional at all times
- Ensure that online activity is related to their professional duty and that personal use should be kept to a minimum
- Ensure that they are not using the school's ICT for financial gain e.g. auction or betting sites
- Ensure that they have read and understood the Computing and related policies
- Be aware that software or hardware should not be installed without prior consent of the Computing Coordinator or head teacher
- Understand that inappropriate use of the school's network may result in some services being removed and further action being taken by the head teacher
- Where data of a personal nature such as school reports, IEPs, correspondence, photographs and assessment data is taken home on a school laptop or other storage device, it must be recognised that this data comes under the Data Protection Act and is subject to the school's Data Protection Policy. Care must therefore be taken to ensure its integrity and security. It **must not be transferred to home computers and should be removed from any portable device including USB pens and memory cards as soon as is practical**.
- Personal devices may be used for note taking in meetings, but under no circumstances used to photograph or record pupils
- School devices can be connected to home networks, providing they are password protected connections.

- Remote access to the school server is used to avoid the need for unscanned and unencrypted USB memory sticks.
- If data is required to be taken off site, you must temporarily sign out an encrypted pen stick, committing to **not** copying the data to your personal computers
- Work can be done on personal computers, however it is strongly advised that a separate, password protected account be created to ensure others cannot access
- If additional equipment is required to be taken off site, e.g. cameras, please sign this off site with the office
- Report any issues to the Senior Management team or ICT Coordinator as soon as possible
- Return any hardware or equipment if they are no longer employed by the school
- Staff must not befriend or contact parents and pupils, including ex pupils under the age of 18, on social networking sites. In the event of networking with parent staff members, professional judgement is advised.
- Staff must not post compromising content (photographs that may cause embarrassment, inappropriate discussions) on social networking site. **Refer to Social Networking Policy**
- Staff must conduct themselves with professional responsibility when online
- Staff must comply with the e-safety policy, especially with reference to the appropriate use of mobile phones in school.

Signed ______________________ Print ___________________ Date ____________