Staff ICT Acceptable Use Policy 2019 - 2020

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner.
This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate policies and the Law.
All staff are expected to:

- Understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, PDAs, digital cameras, iPads, email and social media sites**.**
- School owned information systems must be used appropriately. The Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.
- Understand that any hardware and software provided by school for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, staff will not leave any information system unattended without first logging out or locking their login as appropriate.
- Respect system security and not disclose any password or security information.
- Not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.
- Ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the GDPR Regulation 2018. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online (only within countries or sites with suitable data protection controls) or accessed remotely. Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be encrypted by a method approved by the school.
- Any images or videos of pupils will only be used as stated in the school image use policy and will always take into account parental consent.
- Not keep professional documents which contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile

phones), unless they are secured and encrypted. Where possible any work documents and files will be kept in a password protected environment.

- Protect the devices in my care from unapproved access or theft.
- Not to store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.
- Respect copyright and intellectual property rights.
- Report all incidents of concern regarding children's online safety to the Designated Senior Person (Lisa Gillam or Beverley Munn) as soon as possible. Any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites will be reported to the ICT Coordinator, Matt Harborne, Jatinder Nahal (BM) or the ICT Support Technician as soon as possible who will notify the DSP if necessary.
- Not to attempt to bypass any filtering and/or security systems put in place by the school. If it is suspected that a computer or system has been damaged or affected by a virus or other malware or any school related documents/files have been lost, then this will be reported to the IT Leader as soon as possible.
- Any electronic communications with pupils, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team.
- Use ICT and information systems which are always compatible with their professional role, whether using school or personal systems. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.
- Understand that the use of ICT will not interfere with work duties and will be in accordance with the school's codes of conduct and the Law.
- Understand that creating, transmitting, displaying, publishing or forwarding any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring their professional role, the school, or the LA into disrepute will be dealt with through disciplinary procedures on the advice of HR.
- Promote e-Safety with the pupils in their care and teach them to develop a responsible attitude to safety online, system use and to the content they access or create.
- Any queries or questions regarding safe and professional practice online either in school or off site will be raised with the Head Teacher.
- Understand that their use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security

Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

Review: September 2019

Next review: September 2020