The English Martyrs School and Sixth Form College

STAFF/VOLUNTEER ICT ACCEPTABLE USE POLICY

Policy Reviewed and Adopted by Finance and Resources Committee: October 2015

Version1:1

Date of Next Review: 31st August 2016

Responsible Officer: Stephen Hammond

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. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

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.

1. I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include mobile phones, iPads/MDM's, PDAs, digital cameras, email and social media sites.

2. School owned information systems must be used appropriately. I understand that 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.

3. I understand that any hardware and software provided by my workplace 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, I will not leave any information system unattended without first logging out or locking my login as appropriate.

4. I will respect system security and I will not disclose any password or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system).

5. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the ICT Technical Team.

6. I will ensure that any personal data of students, staff or parents/carers is kept in accordance with the Data Protection Act 1988. 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 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 (where possible) or secured with a password on the folder/file. (Data Security Policy). Any images or videos of students will only be used as stated in the school image use policy (image use policy) and will always take into account parental consent.

7. I will 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. I will protect the devices in my care from unapproved access or theft.

8. I will ensure that all mobile devices have a passcode at all times.

9. I will respect copyright and intellectual property rights.

10. I have read and understood the school policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of students within the classroom and other working spaces.

11. I will report all incidents of concern regarding children's online safety to the e-safety officer and/or the designated person as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the ICT Technical Team and Designated lead person and the e-safety officer as soon as possible.

12. I will not attempt to bypass any filtering and/or security systems put in place by the school, this includes hot-spotting. If I suspect a computer or system has been damaged or affected by a virus or other malware or if I have lost any school related documents or files, then I will report this to the ICT Technical Team as soon as possible.

13. My electronic communications with students, parents/carers and other professionals will only take place via work approved communication channels e.g. via a school provided email address (only used for school business), telephone number. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team.

14. My use of ICT and information systems will always be compatible with my 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. My use of ICT will not interfere with my work duties and will be in accordance with the school AUP and the Law.

15. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role or Academy into disrepute.

16. I will promote e-Safety with the students in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create.

17. I will act in a professional manner at all times when using Social Media ensuring accounts are locked and only accessible via invite (do not accept friend requests from present students). Friend request from past students may be accepted on the understanding that your professional competence is not compromised. Material shared will not be offensive or cause offense in any way.

If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the e-Safety Officer (Pauline Clark) or the Headteacher.

I understand that my 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.

I have read and understood and agree to comply with the Staff ICT Acceptable Use Policy.

Name:

Date: