The Brooksbank School Sports College

E-Safety: Acceptable ICT Use Policy for Staff

Version Number	4.0
Date of Issue	February 2018
Date Approved	February 2018
Date for Review	February 2021
Approved by	Head and Safeguarding Governor
SLT Member Responsible	Director of Finance & Resources

Staff ICT Acceptable Use Policy

(To be read in conjunction with other e-safety policies and the Data Protection Policy)

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.

Use of ICT and information systems should always be compatible with staff's professional role. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites. Staff should ensure that use of ICT does not interfere with their work duties and is in accordance with school policies and the Law.

Staff should ensure that they do 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 their professional role, or the school into disrepute. Staff are also expected to support students to develop a responsible attitude to safety online, system use and to the content they access or create.

ICT Systems
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, 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.

Hardware and software provided by the school is primarily for staff to use to carry out the core business. Staff are expected to use the system responsibly, complying with the requirement to use appropriate passwords and other security measures introduced from time to time. To prevent unauthorised access to systems or personal data, Staff must not leave any information system unattended without first logging out or locking the device as appropriate.

Staff must not download any software or install any hardware without agreement from the Network Manager. If staff suspect a computer or system has been damaged or affected by a virus or other malware they must report this to the ICT support team immediately

Use of personal data:
Personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Bill 2017 and the over-arching European General Data Protection Regulation that comes into force in the UK in May 2018 (see the Data Protection Policy for further detail and be aware that the GDPR has more stringent requirements that need to be complied with). 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.

Staff are reminded that they should only access student personal data via the VLE or Emerge. Any images or videos of pupils will only be used as stated in the school image use policy. Any personal data (including images) stored on portable devices should be properly protected with suitable passwords to prevent un-authorised access.

Staff should not store items of a personal nature on school issued ICT hardware.

Using email for school business

All members of staff are provided with a school email address. Electronic communications with students, parents/carers and other professionals should only take place via work approved communication channels e.g. via a school provided email address or telephone number.

Staff are advised to ensure that business correspondence is received to and sent from the school email address. This is to protect staff's privacy and ensure that business is kept separate from private correspondence.

Monitoring

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 Management believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place there will be a full investigation which could result in disciplinary action taking place.

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.

Staff are asked to report all incidents of concern regarding children's online safety to the Designated Child Protection Coordinator and/or the e-Safety Coordinator as soon as they become aware that there might be a problem. Staff are also asked to report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the e-Safety Coordinator or the Network Manager.

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

Signed: ……...

Print Name: ……..…… Date: …….

Accepted by: …….

Print Name: …… Date: ……