Blenheim

Staff Acceptable Use Agreement

Date Published: May 2019

Expiry Date: May 2021

www.blenheim.surrey.sch.uk

Tel: 01372 745333 Email: headteacher@blenheim.surrey.sch.uk
follow us on Twitter @BlenheimEpsom

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, and to ensure they keep themselves and their professional reputation safe, they are required to read and sign this Acceptable Use Agreement.

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.

- 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, digital cameras, email and social media sites**.**

- 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.

- 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.

- I will respect system security and I will not disclose any password, security information or login, other than to a member of the Network team. I will use a 'strong' password containing numbers, letters and symbols, with 8 or more characters that does not contain a dictionary word or personal information.

- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager. If provided with a Blenheim iPad, I may be able to install my own Apple ID and download my own apps, documents, photos and music, but the school is unable to back these up, and takes no responsibility for data and settings lost as a result of its actions. It is strongly recommended that personal photos are not stored on a school-owned iPad, as there is no guarantee students will not see them.

- I will ensure that any personal data of students, staff or parents/carers is kept in accordance with the Data Protection Act 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, or accessed remotely. Any data that is being removed from the school site (such as via email or on memory sticks or CDs) will be protected by a method approved by the school. I will not store any student data or sensitive school documents in the cloud (eg iCloud or Dropbox). 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.

- I will not keep professional documents that contain school-related sensitive or personal information (including images, files, videos etc.) on any personal devices (such as laptops, digital cameras, mobile phones, iPad). I will upload or download any work documents and files to/from the school network in a password protected environment, eg by using Foldr software. I will protect the devices in my care from unapproved access or theft. If provided with a Blenheim iPad, I will ensure it is protected by a strong passcode at all times and will not take steps to remove the password or installed profiles.

- I will not store any personal information on the school computer system that is unrelated to school activities, such as personal photographs, files or financial information.

- I understand that the IT Services team may remove any non-school information stored on the school network at any time.

- I will respect copyright and intellectual property rights.

- I have read and understood the school e-Safety policy and referred to The Management of e-Safety document as appropriate. These documents cover the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces.

- I will report all incidents of concern regarding children's online safety to one of the Child Protection Liaison Officers (C. Mundy, R. Singleton, S. Harper, J. Glister, T.Smithson, A. Holland, M.Everest, J. Bowden, S. Thornton, J. Preece, H. Peacock) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to L Baker, the Online Safety Administrator, as soon as possible.

- I will not attempt to bypass any filtering and/or security systems put in place by the school. 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 IT Services Team as soon as possible.

- My electronic communications with current or ex 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.

- 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.

- 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, the school, or the Governors, into disrepute.

- I will promote Online-Safety with the pupils 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.

- 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 Online Safety Officer (M. Chalke) or the Head Teacher.

- I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

- I understand that the IT Services team can recall any school device at any time for inspection.

- I understand that it is my responsibility to update any school device with any software updates when they become available. If I am unable to do so I must seek advice from IT Services.

The School may exercise its right to monitor the use of ~~i~~nformation 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.

Useful resources: www.saferinternetcentre.org.uk www.digizen.org/resources/school-staff.aspx

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

Signed: ……..... Print Name: …… Date: …….