

Adult ICT Acceptable Use Policy 2018

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.

- 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, PDAs, digital cameras, email and social media sites.
- Cameras on personal phones will not be used to take pictures of children in any circumstances.
- In the event of a member of staff needing to contact a parent directly, the school office phone will be used.
- 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. Staff may only use school ICT systems for personal use outside of teaching hours, and with the consent of the headteacher. 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 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).
- I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.
- I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with GDPR requirements (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) will be encrypted by a method approved by the school. Secure means of transporting data are either an encrypted memory stick or use of the DLG. Any images or videos of pupils will only be transported by secure media and will always take into account parental consent. Images of pupils will not be stored on personal computers at home.

- 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). Where possible I will use the School Learning Platform to upload any work documents and files in a password protected environment.
- 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 will respect copyright and intellectual property rights.
- I have read and understood the school Online Safety policy which covers 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 the Designated Child Protection Coordinator (Head Teacher) and/or the Online Safety Coordinator (Mrs Suzanne Binks) as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the Online Safety Coordinator (Mrs Suzanne Binks) or the designated lead for filtering (Mr Leonard Lawrence) 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 ICT technician (Mr Leonard Lawrence). I will not open attachments on emails which appear suspicious, this is to reduce the risk of a Ransom attack.
- My 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 and only during working hours. Any pre-existing relationships which may compromise this will be discussed with the Senior Leadership team.
- 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 County Council, into disrepute. This would include any comment made, even in the belief that it is private on a social media site.
- I will promote e-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 Coordinator (Mrs Suzanne Binks).
- I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

Use of cloud based storage (E.G. 2build profile, Tapestry, Fingertips, Class Dojo)

The storage and processing of information and evidence about pupils attainment and or classwork has changed. Some of this information is now captured electronically and stored with an external provider (Data Processor). Please inform (Mrs Cooper DPO) if you wish to opt out of this arrangement.

In addition if those services are not based in the EU (e.g. Class Dojo, Google)

Some apps/services used by the school transfer data to the US. The school will ensure that the company providing the app/service is certified as an approved company under EU-US Privacy Shield. For more information www.privacyshield.gov Please inform (Mrs Sim DPO) if you wish to opt out of this arrangement.

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 GDPR 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.

Signed: Print Name: Date:

Accepted by: Print Name: