



## Staff ICT Acceptable Use Policy 2022-23

***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, tablets, PDAs, 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 or security information. I will use a 'strong' password (A strong password has numbers, letters and symbols, with 15 or more characters, and either does not contain a dictionary word or contains at least two words and is only used on one system).
- I will not attempt to install any purchased or downloaded software, including browser toolbars & video players 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 the Data Protection Act 2018 and UK GDPR. 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 Data Protection policy and will always take into account appropriate consent.

- 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 and encrypted and not stored longer than needed to process. All school data will be removed from my devices upon leaving Astrea employment, it will be shared with relevant colleagues if likely they will require it after my departure. Where possible I will use the Astrea Office 365 based platform to upload any work documents and files in a password protected environment. I will protect the devices in my care from unauthorised access and theft.
- I will not store or process 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 Academy 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 Safeguarding Lead and/or the Data Protection Lead as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the e-Safety Coordinator or the designated lead for filtering 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 Support Provider/Team as soon as possible.
- 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. 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 Trust, into disrepute.
- 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 members of the IT Team or Principal
- I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.
- I will hand back any devices that have been assigned to me and transfer any school information to the ICT Manager upon leaving academy employment. I will ensure that any data (including email accounts) are deleted from both personal and school based devices. I understand that if this is not signed off before my leaving my device/s may be wiped.

*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 Trust's Data Security procedures. 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.*