Staff Online and IT Acceptable Use Policy 2023-24

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 Trust's computer systems in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Technology and the Trust's 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 IT use should be consistent with Astrea's ethos, other appropriate policies, and the Law.

- I have read Part 1 of Keeping Children Safe in Education 2023, including the sections that outline the following topics: nudes and semi-nudes, upskirting, bullying, sexual violence and harassment, and misuse of technology and social media. I understand that these issues can be as damaging to children and adults online, as if they were experienced offline.

- I will follow the guidance in the Astrea Safeguarding and The Academy Online-Safety policies to report any concerns I have regarding online behaviour or risk: I understand the principle of 'safeguarding as a jigsaw' where my concern might complete the picture.

- I understand that Information Systems and IT include networks, data, and data storage, online and offline communication technologies and access devices. Examples include the Internet, mobile phones, tablets, computers, digital cameras, email, and social media sites**.**

- Astrea 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 hardware and software provided by my workplace is intended first and foremost 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 strong passwords which are not shared between systems, including personal accounts.

    - A strong password is a phrase of sufficient complexity and length which prevents guessing or brute force attacks. It should not be a single dictionary word, a common sequence or easily accessible information relating to the user, institution, or service it protects.

    - Passwords should be at least 15 characters long. Long passwords are harder to crack than shorter passwords even if they contain numbers or special characters.

    - Password managers or "three random words" technique are some of the methods of creating strong passwords.

- I will not attempt to modify any equipment or systems provided to me in any way, including installation of software, add-ins, toolbars, etc... or additional hardware, without authorisation from Astrea's IT Team.

- 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 sensitive and/or personal 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 Astrea. 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 the data is secured and encrypted and is not stored longer than needed. All Astrea 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. I will use the Astrea Microsoft 365 platform to upload any work documents and files in a password protected environment as my primary storage location. I will protect the devices in my care from unauthorised access and theft.

- I will not store any personal information on the school/Astrea 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 IT 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 as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the data protection as soon as possible.

- I will not attempt to bypass any filtering and/or security systems put in place by the school or Trust. 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 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 IT 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 IT will not interfere with my work duties and will be in accordance with the school/Trust 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 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 members of the IT Team or Principal.

- I will hand back any devices that have been assigned to me and transfer any school information to the IT Team or Operations/Office 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.

Astrea may exercise its right to monitor the use of ~~i~~information systems, including Internet access, or access to e-mails or any data stored within its IT systems in order to monitor compliance with this or other related Policies and the Trust's data security procedures, or to ensure it can continue providing its services to staff and pupils at a consistent level, or to meet its legal obligations. Where unauthorised and/or inappropriate use of the information system, or unacceptable or inappropriate behaviour may be taking place, Astrea may invoke its disciplinary procedure. If there is a suspicion that the system may be being used for criminal purposes or for storing unlawful digital content, the matter should be brought to the attention of the relevant authority and reported to The Head of IT and Director of Primary Education or Director of Secondary Education.