

Acceptable Use Policy (AUP) for **STAFF, GOVERNORS AND VOLUNTEERS**

What is an AUP?

We ask all children, young people and adults involved in the life of Atlas Academy to sign an Acceptable Use* Policy (AUP), which outlines how we expect them to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms and social media (both when on school site and outside of school).

This AUP is reviewed annually, and I will be asked to sign it upon entry to the Academy and every time changes are made.

Why do we need an AUP?

All staff, governors and volunteers have particular legal / professional obligations and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum, and it is everybody's responsibility to uphold the Academy's approaches, strategy and policy as detailed in the full Online Safety Policy.

Where can I find out more?

All staff, governors and volunteers should read Atlas Academy's full Online Safety Policy for more detail on our approach to online safety and links to other relevant policies (e.g. Safeguarding Policy, Behaviour Policy, etc).

If you have any questions about this AUP or our approach to online safety, please speak to the Principal or a member of the Safeguarding Team.

What am I agreeing to?

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 Academy'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.

1. This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the Academy 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.
- Academy 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 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 the Data Protection Act 1988. 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 Academy image use policy and will always take into account parental consent.
- I will not keep professional documents which contain Academy-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. Where possible I will use the Academy's remote network access facility to upload any work documents and files in a password protected environment. I will protect the devices in my care from unapproved access or theft.
- I will not store any personal information on the Academy 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 Safeguarding Lead as soon as possible.
- I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the Designated Safeguarding Lead as soon as possible.
- I will not attempt to bypass any filtering and/or security systems put in place by the Academy. If I suspect a computer or system has been damaged or affected by a virus or



other malware or if I have lost any Academy related documents or files, then I will report this 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 an Academy provided email address or telephone number. Any pre-existing relationships which may compromise this will be discussed with the Principal.
- My use of ICT and information systems will always be compatible with my professional role, whether using Academy 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 Academy Online Safety Policy, 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 Academy, or Astrea Academy 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 the Designated Safeguarding Lead or the Principal.
- I understand that my use of the information systems, the 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 Academy information to the Academy's systems upon leaving Atlas Academy employment. I will ensure that any data (including email accounts) are deleted from both personal and Academy based devices. I understand that if this is not signed off before my leaving my device/s may be wiped.

The Academy 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 Academy'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 Academy will invoke its disciplinary procedure. If the Academy 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 understand that breach of this AUP and/or of the Academy's full Online Safety Policy may lead to appropriate staff disciplinary action or termination of my relationship with the Academy and where appropriate, referral to the relevant authorities



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

Signed:

Print Name:

Date:

Accepted by:

Print Name: