Technology acceptable use agreement – staff, volunteers, contractors and visitors

The Aspire Educational Trust (AET) **January 2022**

Whilst our trust promotes the use of technology and values the positive effects it can have on enhancing pupils' learning and community engagement. We highly value the important role staff play in protecting the trust and its schools from potential cybersecurity risks and as such recognise the importance of supporting colleagues with appropriate training and guidance. We must also ensure that staff use technology appropriately. Any misuse of technology will not be taken lightly and will be reported in order for any necessary further action to be taken.

This acceptable use agreement is designed to outline staff responsibilities and the practical steps you should take to protect yourself and our trust when using technology, whether this is via personal devices or school/trust devices, or on/off the trust's premises, and applies to all staff, volunteers, contractors and visitors.

The Aspire Educational Trust guidance for safety in remote online video and telephone communication with pupils and parents document is available to all staff. The guidance has been written to help keep staff and pupils safe when using technology.

It is strongly advised that you always seek advice from your principal or IT support provider if you are unsure about any aspect of using technology safely and appropriately. We believe it is important that everyone feels comfortable speaking out if they feel that something isn't right.

Please read this document carefully and click the green read button to show you agree to the terms outlined.

1. **Using technology**

- I will only use IT systems, such as computers (including laptops) and tablets, which have been permitted for my use by the principal or trust line manager.
- I will ensure any authorised personal device is protected by up to date anti-virus software and operating system, a strong password, an enabled firewall and is set to receive updates automatically. [School-owned devices' systems and updates should be managed by the school's IT support provider. The IT support provider can help you to check your authorised personal devices meet trust requirements].
- I will not ignore software updates.
- If I see error messages or believe software or apps aren't updating I will contact the school or trust's IT support.
- I will not install any software onto school IT systems unless instructed to do so by the e-safety lead or principal.
- I will keep devices physically secure at all times.
- I will secure devices with a screen lock.
- I will use strong passwords.

- I will store passwords securely.
- I will use separate passwords for personal and work accounts.
- I will reset work accounts with new passwords if I suspect my password has been exposed or breached.
- I will not share school-related passwords with pupils, other staff or third parties.
- I will only use the approved email accounts that have been provided to me by the school or trust.
- I will not use personal emails for school or trust related business.
- When using technology, I will ensure that any personal data, including sensitive personal data, is processed in line with the UK GDPR and AET policies.
- I will delete any chain letters, spam and other emails from unknown sources without opening them.
- I will ensure that I obtain permission prior to accessing learning materials from unapproved sources.
- I will only download apps on school-owned devices from official sites (like Google Play or Apple App Store).
- I will carefully read the permissions information when installing an app to check if they are accessing school data. If they do, I will ensure this is necessary and permitted.
- I will only use trust or school issued encrypted removable media (USB) when necessary and will keep this securely stored in line with the UK GDPR.
- I will return removable media to the e-safety lead for safe disposal once I am finished with it.
- When delivering remote online learning I will follow the agreed guidance, policies and procedures of the academy/trust.
- I will only use the internet for personal use during out-of-school hours, including break and lunch times.
- I will not search for, view, download, upload or transmit any explicit or inappropriate material when using the internet.

2. Mobile devices

- I will only use school-owned mobile devices for educational purposes.
- I will only use personal mobile devices for personal business during out-of-school hours, including break and lunch times.
- If, in exceptional circumstances, I need to use a personal device at other times I will seek permission from the principal first.
- I will ensure that personal mobile devices are either switched off or set to silent mode during school hours and will only make or receive calls in the school's specified areas.
- I will ensure personal mobile devices are stored securely, as determined by the school, during lesson times.
- I will ensure personal mobile devices stored in pupil areas are internet disabled during lesson times.
- I will not use personal mobile devices to take images or videos of pupils or staff.
- If, in exceptional circumstances, it is necessary to use a personal device for school business I will seek permission from the principal first.

- I will use school-owned mobile devices to take images or recordings of pupils and staff.
- I will not use mobile devices to send inappropriate messages, images or recordings.
- I will ensure that personal and school-owned mobile devices do not contain any inappropriate or illegal content.
- I will not access the WiFi system using personal mobile devices, unless permission has been given by the principal.
- I will not use personal mobile devices to communicate with pupils or parents.
- If, in exceptional circumstances, it is necessary to use a personal device for school business I will follow the agreed guidance, policies and procedures of the academy/trust.
- I will not store any images or videos of pupils, staff or parents on any mobile device unless consent has been sought from the individual(s) in the images or videos.
- In line with the above, I will only process images or videos of pupils, staff or parents for the activities for which consent has been sought.
- I will ensure that any school data necessarily stored on personal mobile devices is encrypted and pseudonymised and give permission for the e-safety lead to erase and wipe data off my device if it is lost or as part of exit procedures.

3. Social media and online professionalism

- If I am representing the school online, e.g. through blogging or on school social media account, I will express neutral opinions and will not disclose any confidential information regarding the school, or any information that may affect its reputability.
- I will not use any school-owned mobile devices to access personal social networking sites.
- I will not communicate with pupils or parents over personal social networking sites.
- I will not accept 'friend requests' from any pupils or parents over personal social networking sites.
- I will inform the principal of any personal friendships with a parent where this exists beyond the usual parent/professional relationships and may impact on aspects of my compliance with the requirements of this acceptable use agreement.
- I will ensure that I apply the necessary privacy settings to any social media, professional networking sites and app accounts.
- I will not publish any comments or posts about the school/trust on any social networking sites which may affect the school/trust's reputability.
- I will not post or upload any defamatory, objectionable, copyright infringing or private material, including images and videos of pupils, staff or parents, on any online website.
- I will not post or upload any images and videos of pupils, staff or parents on any online website without explicit consent from the individual(s) in the images or videos.
- In line with the above, I will only post images or videos of pupils, staff or parents for the activities for which consent has been sought.

- I will not give my home address, phone number, mobile number, social networking details or personal email addresses to pupils or parents – any contact with parents will be done through authorised school/trust contact channels.

4. Working at home

- I will adhere to the principles of the UK GDPR when taking work home or working off site.
- I will ensure I obtain permission from my line manager and data protection officer (DPO) before any personal data is transferred from a school-owned device to a personal device.
- I will ensure any personal data transferred from a school-owned device to a personal device is encrypted or pseudonymised.
- I will ensure any sensitive personal data is not transferred to a personal device unless completely necessary – and, when doing so, that it is encrypted.
- I will ensure my personal device has been assessed for security by the e-safety lead or IT support provider before it is used for lone/home-working.
- I will ensure no unauthorised persons, such as family members or friends, access school or trust business on personal devices used for lone/home-working.
- I will act in accordance with the trust's E-Security Policy when transporting school/trust equipment and data.

5. Training

- I will ensure I participate in cyber-security, online or data protection training.
- I will ensure I employ methods of good practice and act as a role model for pupils when using the internet and other digital devices.

6. Reporting misuse, suspicious activity or data breaches

- I will ensure if I have any doubt about suspicious activity on any of my accounts or devices that I will report it immediately.
- I understand my responsibility to adhere to the trust's data protection policies and to report all online data breaches immediately.
- I understand that my use of the internet will be monitored and recognise the consequences if I breach the terms of this agreement.
- I understand that the principal or my line manager may decide to take disciplinary action against me in accordance with the Disciplinary Policy and Procedure, if I breach this agreement.

By clicking 'read' on Compliance Manager in relation to this document you are electronically recording the following:

I certify that I have read and understood this agreement and ensure that I will abide by each principle.

Agreement Updated 07/01/2021

Changes

- Removed academic year date and replaced with date of this version. Removes requirement for all staff to reread annually if no changes are made at review.
- Reference to The Aspire Educational Trust Guidance for Safety in Remote Online Video and Telephone Communication with Pupils and Parents
- Slight wording changes to reflect;

    - Introduction of remote online learning
    - Increased possibility of staff being required to use personal devices if working from home
    - Increased probability that staff will be required to make regular contact with pupils using technology when school is working remotely due to lockdown or absence.

Updated 11/01/2022

Changes

- Changed date of agreement
- Removed requirements that member of staff is unable to control or did not relate to their own actions.
- Introduced requirements that align with the NCSC Cyber security training for staff, completed by all staff Spring 2022.