

Device and technology acceptable use agreement for – staff, volunteers, contractors and visitors

The Aspire Educational Trust

September 2025

Whilst our trust promotes the use of technology or devices, and understands the positive effects they can have on enhancing pupils' learning and community engagement, we must also ensure that staff use technology and devices appropriately. Any misuse of technology and devices will not be taken lightly and will be reported to the principal in order for any necessary further action to be taken.

This agreement outlines staff members' responsibilities when using technology and devices, both school-owned and personal, and applies to all staff, volunteers, contractors and visitors.

The trust may undertake monitoring activities of employees for safeguarding and security purposes. The trust will ensure that any monitoring activities undertaken are lawful and fair to workers, as well as meet data protection requirements.

If any monitoring activities are undertaken, then the trust will ensure that employees are made aware of the nature, reasons, and extent of the monitoring, that the monitoring has a lawful basis, clearly defined purpose, and that it is as unintrusive as possible to the employees.

Please read this document carefully, click to confirm as read and to show you agree to the terms outlined.

Data protection and cyber-security

I will:

- Use technology and devices, including the use and storage of personal data, in line with data protection legislation, including the Data Protection Act 2018 and UK GDPR.
- Follow the trust's Data Protection Policy and any other relevant trust/school policies and procedures.

I will not:

- Attempt to bypass any filtering, monitoring and security systems.
- Share school-related passwords with pupils, staff, parents or others unless permission has been given for me to do so in exceptional circumstances.

Using technology in school

I will:

- Follow the Staff ICT and Electronic Devices Policy.
- Only use ICT systems which I have been given permission to use.
- Ensure I obtain permission prior to accessing materials from unapproved sources.
- Only use the school's internet for personal use during out-of-school hours, including break and lunch time.

- Only use school approved encrypted removable media and keep this securely stored.
- Follow the agreed guidance, policies and procedures of the trust when delivering remote online learning.

I will not:

- Install any software onto school ICT systems unless instructed to do so by the principal or IT support technician.
- Search for, view, download, upload or transmit any inappropriate material when using the internet.

Emails

I will:

- Only use the approved trust/school email accounts that have been provided to me when sending communications regarding school business.
- Ensure any personal information that is being sent via email is only sent to the relevant people and is appropriately protected.

I will not:

- Use personal emails to send and/or receive school-related personal data or information, including sensitive information.
- Use personal email accounts to contact pupils or parents.

School-owned devices

I will:

- Only use school-owned devices for the purpose of carrying out my school responsibilities.
- Only access websites and apps that have been approved by the principal.
- Understand that the usage of my school-owned devices will be monitored.
- Keep my school-owned devices physically secure at all times.
- Provide suitable and secure care for my school-owned devices at all times.
- Secure devices with a screen lock.
- Use strong passwords.
- Use separate passwords for personal and work accounts.
- Reset work accounts with new passwords if I suspect my password has been exposed or breached.
- Not share school-related passwords with pupils, other staff or third parties.
- Only communicate with pupils and parents on school-owned devices using appropriate channels.
- Ensure I promptly install and update security software on school-owned devices as directed by the principal or IT support technician.
- Only download apps on school-owned devices from official sites (like GooglePlay or Apple App Store) and with the permission of the principal.
- 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.
- Seek permission from the principal before using a school-owned device to take and store photographs or videos of pupils, parents, staff and visitors.
- Immediately report any damage or loss of my school-owned devices to the principal.

- Immediately report any security issues, such as downloading a virus or receiving a potential phishing email to the principal and IT support technician.
- Understand that I may be expected to pay an excess for any repair or replacements costs where the device was damaged or lost as a result of my own negligence.
- Make arrangements to return all school-owned devices to the principal at the end of my employment at the school.

I will not:

- Permit any other individual to use my school-owned devices, unless otherwise agreed by the principal.
- Install any software onto school-owned devices unless instructed to do so by the principal or IT support technician.
- Use school-owned devices to send inappropriate messages, images, videos or other content.
- Use school-owned devices to view, store, download or share any inappropriate, harmful or illegal content.
- Use school-owned devices to access personal social media accounts.

Personal devices

I will:

- Only use personal devices during out-of-school hours, including break and lunch times.
- Seek permission from the principal first if, in exceptional circumstances, I need to use a personal device at other times.
- Ensure personal mobile devices are either switched off or set to silent mode during school hours and will only make or receive calls in specific areas, in accordance with the school's policy.
- Store personal devices appropriately during school hours, in accordance with the school's policy.
- Ensure personal mobile devices stored in pupil areas are internet disabled during lesson times.
- Understand that I am liable for any loss, theft or damage to my personal devices.

I will not:

- Use personal devices to communicate with pupils or parents.
- Access the school's Wi-Fi using a personal device unless permission to do so has been granted by the principal.
- Use personal devices to take photographs or videos of pupils or staff.
- Store any school-related information on personal devices unless permission to do so has been given by the principal.

Social media and online professionalism

I will:

- Follow the trust's Social Media Policy.
- Understand that I am representing the school and behave appropriately when posting on trust or school social media accounts.
- Ensure I apply necessary privacy settings to social media accounts.

I will not:

- Communicate with pupils or parents over personal social media accounts.
- Accept 'friend' or 'follow' requests from any pupils or parents over personal social media accounts.
- Post any comments or posts about the trust or school on any social media platforms or other online platforms which may affect the trust or school's reputability.
- Post any defamatory, objectionable, copyright-infringing or private material, including images and videos of pupils, staff or parents, on any online website.
- Post or upload any images and videos of pupils, staff or parents on any online website without consent from the individuals in the images or videos.
- Give my home address, phone number, mobile number, social networking details or email addresses to pupils or parents – any contact with parents will be done through authorised school contact channels.

Working from home

I will:

- Use a school-owned device whenever possible when working from home.
- Ensure I obtain permission from the principal before any personal data is transferred from a school-owned device to a personal device.
- Ensure any data transferred from a school-owned device to a personal device is encrypted or pseudonymised.
- Ensure any sensitive personal data is not transferred to a personal device unless completely necessary – and, when doing so, that it is encrypted.
- Ensure my personal device has been assessed for security by the IT support technician before using for home working.
- Ensure no unauthorised persons, such as family members or friends, access school related information on any personal or school devices used for home working.

Training

I will:

- Participate in any relevant training offered to me, including cyber-security, use of email and online safety.
- Allow principal and/or DPO to undertake regular audits to identify any areas of need I may have in relation to training.
- Employ methods of good practice and act as a role model for pupils when using the internet and other digital devices.

Reporting misuse

I will:

- Report any misuse by pupils or staff members breaching the procedures outlined in this agreement to the principal.
- Understand that my use of the internet will be monitored by the principal and recognise the consequences if I breach the terms of this agreement.
- Understand that the principal may decide to take disciplinary action against me, in accordance with the Disciplinary Policy and Procedure, if I breach this agreement.

Monitoring workers

I understand that:

- The school will notify employees when monitoring takes place and will conduct its monitoring activities with transparency, clearly explaining how and why they process my information.

- The school will conduct its monitoring activities in a way that's accountable and compliant with UK GDPR.
- Monitoring is used mainly for security and safeguarding purposes.
- Monitoring technologies may include, but aren't limited to, CCTV, webcams, electronic sign-in systems.
- I can access the information collected by the school by making a subject access request (SAR).
- The school will carry out a data protection impact assessment (DPIA) prior to undertaking their monitoring activities. Completing a DPIA identifies and minimises any potential risks that come with monitoring activities.

By clicking 'read' on the National College 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.