**What is an AUP (Acceptable Use Policy)?**

An Acceptable Use Policy sets out the roles, responsibilities and procedures for the acceptable, safe and responsible use of all technologies to safeguard adults, children and young people within a school or other educational setting. The policy recognises the ever-changing nature of emerging technologies and highlights the need for regular review to incorporate development within an area. At present the internet technologies used extensively by young people in both home and school environments include:

- Websites/blogs
- Social networking and chat rooms
- Gaming/forums on Xbox live etc.
- Music downloading
- Mobile phones with wireless connectivity
- Email and instant messaging
- Learning platforms
- Video broadcasting
- Apple/Windows apps

Despite there being significant educational and social benefits associated with the use of these technologies, there are risks which need to be emphasised to all users and steps taken to safeguard against them. This policy should also provide support and guidance to parents/carers and the wider community (where appropriate) for the safe and responsible use of these technologies beyond the school or educational setting. It explains procedures for any unacceptable use of these technologies by adults, children or young people.

**Why have an AUP?**

The use of the internet as a tool to develop learning and understanding has become an integral part of school and home life. There are always going to be risks to using any form of communication which lies within the public domain. Therefore, it is imperative that there are clear rules, procedures and guidelines to minimise those risks whilst children access these technologies.

The risks include:

- Commercial issues with spam and other inappropriate e-mail
- Online grooming
- Illegal activities of downloading or copying any copyright materials and file-sharing via the internet or any mobile device
- Viruses
- Cyber-bullying
- Sexting-the sending of indecent personal images, videos or text via mobile phones for private viewing- these can potentially be widely distributed and publicly viewed
- On-line content which is abusive or pornographic

It is also important that adults are clear about the procedures, for example, only contacting children and young people about homework via a school e-mail address, not a personal one, so that they are also safeguarded from misunderstandings or allegations through a lack of knowledge of potential risks.

Whilst the school or setting should acknowledge that every effort will be made to safeguard against all risks, it is likely that they will never be able to completely eliminate them. Any incidents that may arise should be dealt with quickly and according to policy to ensure children and young people continue to be protected.

Where possible, another member of staff should be copied into emails to also reduce risks. There is also a responsibility to educate parents about the risks and how this is managed inside school, along with what they can do at home to help safeguard their child.

**Aims**

- To emphasise the need to educate staff, children and young people about the pros and cons of using new technologies both within and outside school or other educational settings.
- To provide safeguards and rules for acceptable use to guide all users, whether staff or student, in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the school or educational setting.
- To develop links with parents/carers and the wider community ensuring input into policies and procedures with continued awareness of the benefits and potential issues related to technologies.

**Device and technology acceptable use agreement for staff**

Whilst our school 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 headteacher 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 school may undertake monitoring activities of employees to ensure the quality and quantity of work. The school 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 school will ensure that employees are made aware of the nature, reasons, and extent of the monitoring, that the monitoring has a clearly defined purpose, and that it is as unintrusive as possible to the employees.

Information which is gathered from monitoring activities must have a lawful basis. The school understands rights and the private lives of workers, particularly as remote working excessive monitoring can have adverse impacts continues to become more common, that excessive monitoring can have adverse impacts on data protection rights and the private lives of workers, particularly as remote working continues to become more common.

The school will ensure that the monitoring of workers is necessary for the identified reasons. The school will also ensure that all suitable safety checks are carried out prior to monitoring activities.

Please read this agreement carefully, and sign at the bottom 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 school's Data Protection Policy and any other relevant 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.

**Using technology in school**

I will:

- Follow the Staff ICT and Electronic Devices Policy.
- Only use ICT systems which I have been permitted to use.
- Ensure I obtain permission prior to accessing materials from unapproved sources.
- Only use the internet for personal use during out-of-school hours, including break and lunch time.
- Only use recommended removable media and keep this securely stored.

I will not:

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

**Emails**

I will:

- Only use the approved 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 headteacher.
- Understand that the usage of my school-owned devices will be monitored.
- Keep my school-owned devices with me or within my sight at all times.
- Transport school-owned devices safely.
- Provide suitable care for my school-owned devices at all times.
- Only communicate with pupils and parents on school-owned devices using appropriate channels.
- Ensure I install and update security software on school-owned devices as directed by the ICT technician.
- Seek permission from the headteacher 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 ICT technician.
- Immediately report any security issues, such as downloading a virus, to the ICT technician or headteacher.
- Understand that I am 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 school-owned devices to the ICT technician upon the end of my employment at the school.

I will not:

- Permit any other individual to use my school-owned devices without my supervision, unless otherwise agreed by the headteacher.
- Install any software onto school-owned devices unless instructed to do so by the headteacher or ICT 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.
- Ensure personal devices are either switched off or set to silent mode during school hours.
- Only make or receive calls in specific areas, e.g. the staff room.
- Store personal devices appropriately during school hours, e.g. a lockable cupboard in the classroom.
- 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 headteacher or ICT technician.
- 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 headteacher.

**Social media and online professionalism**

I will:

- Follow the school's Social Media Policy.
- Understand that I am representing the school and behave appropriately when posting on 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 school on any social media platforms or other online platforms which may affect the 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:

- Ensure I obtain permission from the headteacher and DPO 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 DPO and ICT technician before it is used for home.
- Ensure no unauthorised persons, such as family members or friends, access any personal devices used for home working.

**Training**

I will:

- Participate in any relevant training offered to me, including cyber-security and online safety.
- Allow the ICT technician and 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.
- Deliver any training to pupils as required.

**Reporting misuse**

I will:

- Report any misuse by pupils or staff members breaching the procedures outlined in this agreement to the headteacher.
- Understand that my use of the internet will be monitored by the ICT technician and recognise the consequences if I breach the terms of this agreement.
- Understand that the headteacher 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 that the school will clearly explain what personal information of mine is collected and how it's utilised and maintained.
- Monitoring is often used for security purposes, managing employees' performance, and monitoring sickness and attendance.
- Monitoring technologies include, but aren't limited to, camera surveillance, webcams, technologies for timekeeping and keyboard activity, productivity tools, internet activity trackers, body-worn devices, and hidden audio recording.
- Personal data relating to myself which is collected from monitoring activities is securely kept and protected and isn't kept for any longer than necessary by the school.
- The school will factor in increased expectations of privacy if I work from home.
- The school will conduct its monitoring activities in a way that's fair and reasonably expected.
- The school 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.
- I can object to having my personal information collected and processed if the lawful basis which the school is relying on is a public task or legitimate interests based on my personal situation.
- The school may refuse to comply with the objection if they can demonstrate that the monitoring is for legitimate interests which override my interests, rights, and freedoms, or that the monitoring is for establishment, exercise, or defence of legal claims.
- Tools for monitoring workers continue to become increasingly sophisticated, and that the school will inform me if they choose to use solely automated processes for monitoring activities.

- 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.

**Agreement**

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

| | |
|---|---|
| **Name** | |
| **Signature** | |
| **Date** | |