Electronic Information and Acceptable Use Policy

Date last reviewed and approved:	**September 2025**
Due for Review:	**September 2027**

This policy covers the following aspects of Acceptable Use in relation to e-safety for all school staff, volunteers, visitors and pupils:

- **Use of school-based equipment**
- **Social Networking**
- **Managing digital content**
- **Email**
- **TEAMs**
- **Mobile phones and devices**
- **Learning and teaching**

Use of school based equipment

When using the school's ICT equipment and other information systems, I have understood and will comply with the following statements

- I will access the internet and other ICT systems using an individual username and password, which I will keep secure. I will ensure that I log out after each session and never allow other users to access the internet through my username and password. I will report any suspicion, or evidence that there has been a breach of my personal security in relation to access to the internet or ICT systems, to the e-safety lead or headteacher.
- All passwords I create will be in accordance with the school e-safety Policy. I will ensure that I use a suitably complex password for access to the internet and ICT systems.
- I will not share my passwords.
- I will seek consent from the e-safety lead prior to the use of any new technologies (hardware, software, cloud-based services) within school.
- I will not search for, download, upload or forward any content that is illegal or that could be considered an offence by another user. If I encounter any such material I will report it immediately to the e-safety lead or headteacher.
- I will take a professional and proactive approach to assessing the effectiveness of the internet content-filtering platform in relation to the educational content that can be viewed by the pupils in my care.
- I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, I will report this to the e-safety lead/headteacher.
- I understand my personal responsibilities in relation to the Data Protection Act and the privacy and disclosure of personal and sensitive confidential information.
- I will take reasonable precautions to ensure that any devices (laptops, tablets, cameras, removable media or phones) are stored in a secure manner when taken off site (car / home/ other location). Devices will not be stored in a car overnight or left in sight when not in use, e.g. by an open window or on the back seat of a car.
- I will only use school-owned or provided portable storage (USB sticks, SSD cards, portable hard drives etc).
- I will ensure that any personal or sensitive information taken off site will be situated on a school-owned device with appropriate technical controls such as encryption/ password protection deployed.
- Any information asset, which I create from other information systems, which could be deemed as personal or sensitive will be stored on the school network and access controlled in a suitable manner in accordance with the school data protection controls. (For example spread sheets/other documents created from information located within the school information management system).
- I will not download or install any software from the internet or from any other media which may compromise the school network or information situated on it without prior authorisation from the e-safety lead or headteacher.
- I understand that the use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990 and breaches will be reported to the appropriate authorities.
- I understand that my files, communications and internet activity may be monitored and checked at all times to protect my own and others' safety, and action may be taken if deemed necessary to safeguard me or others.

Social Networking

- I must not talk about my professional role in any capacity when using personal social media such as Facebook, Instagram and YouTube or any other online publishing websites.
- I must not use social media tools to communicate with current or former pupils under the age of 18.
- I will not use any social media tools to communicate with parents unless approved in writing by the Head Teacher.
- I will set and maintain my profile on social networking sites to maximum privacy and give access to known friends only.
- Staff must not access social networking sites for personal use during school hours.
- If I experience any derogatory or slanderous comments relating to the school, colleagues or my professional status, I will take screenshots for evidence and escalate to the e-safety coordinator.

Managing digital content

- I will demonstrate professional, safe and responsible behaviour when creating, using and storing digital images, video and sound within school.
- I will only use school equipment to create digital images, video and sound. Digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress. No resources will be published online without the permission of the staff and pupils involved as detailed in the e-safety Policy.
- Under no circumstances will I use any personally-owned equipment for video, sound or images without prior consent from a member of the Senior Leadership Team.
- When searching for images, video or sound clips, I will ensure that I or any pupils in my care are not in breach of any copyright licencing.
- I will ensure that any images, videos or sound clips of pupils are stored on the school network and never transferred to personally-owned equipment.
- I will ensure that any images taken on school-owned devices will be transferred to the school network and deleted as soon as possible from the memory card.
- I will model safe and responsible behaviour in the creation and publishing of online content within the school learning platform and any other websites. In addition to this I will encourage colleagues and pupils to adopt similar safe behaviour in their personal use of blogs, wikis and online publishing sites.

Email

- I will use my school email address for all correspondence with staff, parents or other agencies and I understand that any use of the school email system will be monitored and checked. I will under no circumstances use my private email account for any school-related business.
- Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.
- I will ensure that any posts made on websites or via electronic communication, by either myself or the pupils in my care, will not damage the reputation of my school.
- I will seek permission if I need to synchronise any school email account with a personally-owned handheld device.
- I will take care in opening any attachments sent by email. I will only open emails and associated attachments from trusted senders.
- Emails sent to external organisations will be written carefully and if necessary authorised before sending to protect myself. As and when I feel it necessary, I will carbon copy (cc) the head teacher, line manager or another suitable member of staff into the email.
- I will ensure that I manage my email account, delete unwanted emails and file those I need to keep in subject folders.
- I will access my school email account on a regular basis to ensure that I respond in a timely manner to communications that require my attention.

Use of Microsoft TEAMs

Microsoft Teams is provided by the school as a secure online learning and communication platform. It is to be used for educational purposes only, in line with our school values and safeguarding responsibilities.

Expectations for Staff

- I will use Teams as a professional platform for teaching, learning, and communication.
- I will maintain safeguarding standards by ensuring appropriate language, conduct, and use of video/audio.
- I will ensure that any recorded lessons or meetings follow GDPR and data protection policies.
- I will only use Teams outside of direct teaching time and not as an instant messaging service.
- I will ensure that the settings on my Teams account are in line with GDPR policies.
- I will not use Teams for any form of bullying, harassment, or inappropriate behaviour.
- I will not use Teams for any personal or non-school-related work.
- I understand that breaches of this policy may result in restricted access or disciplinary action.

Mobile phones and devices

- I will ensure that my mobile phone and any other personally-owned device is switched off or switched to 'silent' mode during school hours.
- Bluetooth communication should be 'hidden' or switched off and mobile phones or devices will not be used during teaching periods unless permission has been granted by a member of the Senior Leadership Team in emergency circumstances.
- I will not contact any parents or pupils on my personally-owned device.
- I will not use any personally-owned mobile device to take images, video or sound recordings.

Learning and teaching

- In line with every child's legal entitlement I will ensure I teach age an appropriate e-safety curriculum.
- I will support and promote the school e-safety policy at all times. I will model safe and responsible behaviour in pupils when using ICT to support learning and teaching.
- I will ensure that I am aware of my individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.
- I understand the importance of respecting and acknowledging copyright of materials found on the internet and will model best practice in the creation of my own resources at all times.

Appendix 1. AUP Policy Appendix on the Use of Mobile Phones in School

While mobile phones and personal communication devices are commonplace in today's society, it is recognised that personal mobile phones have the potential to be used inappropriately.

Effective guidance is in place to avoid the use of mobile phones causing unnecessary disruptions and distractions within the workplace, and to ensure effective safeguarding practice is promoted to protect against potential misuse.

Most mobile phones now offer Internet and email access, alongside messaging, camera, video and sound recording. Mobile phones alongside other forms of technology are changing the way and speed in which we communicate. They can provide security and reassurance; however there also associated risks. Safeguarding of children within the school is paramount.

School staff:

Staff may wish to have their personal mobile phones at work for use in case of emergencies, however there is a clear expectation that all personal use is limited to areas and times when there are no children present, or likely to be present.

1. The school expects staff to lead by example. Other than in agreed exceptional circumstances, mobile phones should be switched off or on silent and left in a safe place during lesson times.
2. Staff should not contact pupils or parents from their personal mobile phone in or out of school time, or give their mobile phone number to pupils or parents. If a member of staff needs to make telephone contact with a pupil, a school telephone should be used.
3. Staff should never send to, or accept from, colleagues or pupils, texts or images that could be viewed as inappropriate
4. Staff are not permitted to take photos or videos of pupils. If photos or videos are being taken as part of the school curriculum or for a professional capacity, the school equipment will be used for this. Staff should not allow themselves to be photographed by a pupil(s).
5. In circumstances such as outings and off site visits, staff will agree with the HT or DHT the appropriate use of personal mobile phones in the event of an emergency.
6. This guidance should be seen as a safeguard for members of staff and the school. Any breach of school policy may result in disciplinary action against that member of staff.

Pupils:

Primary

Pupils are dissuaded from bringing mobile phones to school. If it is deemed necessary for a pupil to bring a mobile phone to school, (e.g. in the case of older pupils because they travel to and from school independently), then the expectation is that the pupil hands their phone in to the class teacher.

Parents, visitors and contractors:

Parents, visitors and contractors are respectfully requested not to use their mobile phones at all on the school site. Should phone calls and/or texts need to be taken or made, use is restricted to those areas not accessed by children. To avoid any unnecessary disturbance or disruption to others, should phone calls/and or texts need to be taken or made, visitors are asked to leave the premises to do so or ask at the office where they can do this.

Photos of children must only be taken on school devices and in accordance with the school's 'Safe use of Children's Images policy' and in accordance with the General Data Protection Regulations (GDPR) and the Data Protection Act 2018

Any individual bringing a personal device into the school must ensure that it contains no inappropriate or illegal content.

Inappropriate or illegal content:
Where there is a suspicion that the material on a mobile phone may be unsuitable and may constitute evidence relating to a criminal offence, the 'Allegations of Abuse' process will be followed (please refer to the school's 'Safeguarding and Child Protection Policy').

Staff, students or volunteers remain responsible for their own property and will bear the responsibility of any losses.

Related Policies and guidance:

Safeguarding and Child Protection Policy (September 2023)

Guidance for Safer Working Practice for Adults who work with Children and Young People in Education Settings (April 2020)

Keeping Children Safe in Education (September 2023)

Guidance for schools and other establishments on the use of images (July 2019)

Data Protection: A toolkit for schools, DfE, (August 2018)