

Winchester House School
Staff Acceptable Use Policy

Last reviewed: 1st September 2026 (DSL / Deputy Head Pastoral)

Adopted by Governors:

Next review due: 1st September 2027 (DSL / Deputy Head Pastoral)

Scope

This Acceptable Use Policy (AUP) should be read alongside the School's Online Safety and Digital Awareness Policy, Staff Code of Conduct, Data Protection Policy and Safeguarding and Child Protection Policy.

It applies to all those who work at Winchester House School, including academic staff, support staff, governors, volunteers, GAP students and anyone provided with access to the School's IT systems. The scope of this document includes the use of personal devices as well as school-owned equipment and applies equally to the use of School systems accessed remotely.

The purpose of this AUP is to ensure that staff are safe, responsible, professional and secure users of technology. By adhering to the principles in this agreement, staff should be able to minimise risks to their own safety, the safety of others, and the safety and security of Winchester House School's IT systems.

Principles

Use of School Equipment and Systems

- Staff must report any broken, damaged or potentially unsafe IT equipment as soon as possible to prevent further damage and/or injury to others.
- Staff must not share passwords, authentication details or account credentials for any School IT system with anyone else.
- Staff must comply with the School's security requirements, including the use of strong passwords and Multi-Factor Authentication (MFA) where required.
- Staff shall not knowingly download, install or attempt to install software, applications or programs that have not been authorised by the School, as these may compromise the security or stability of School devices, systems or networks.
- Staff shall not examine, access, change or use another person's files, output, account or username without explicit authorisation.
- School data must not be downloaded, stored or transferred to unauthorised personal devices, storage media or cloud services.
- Staff must ensure the safe handling, storage and sharing of personal data and act in accordance with the School's Data Protection Policy, Staff Code of Conduct and other relevant School policies and procedures.
- Staff shall only use their Winchester House email account for School-related purposes and must ensure that all communications are professional in tone and manner.
- Staff must use School-provided devices when contacting pupils or parents/carers during off-site activities, educational visits or residential trips wherever reasonably practicable. Where contact information is stored on a School device for the purpose of a visit, it must be deleted once no longer required.
- If a pupil requires the use of a mobile device during an educational visit or off-site activity, a School device should be used wherever possible. Where no School device is available, a member of staff may permit the supervised use of their own device, ensuring appropriate safeguarding, privacy and professional boundaries are maintained at all times.

Use of the Internet and Web Technologies

- Staff must not use the internet for personal reasons whilst supervising pupils or during direct contact time.
- Limited personal use of the internet is permitted during non-contact time, such as breaks and lunch periods, provided that it is lawful, appropriate and consistent with the School's standards of professional conduct. Personal use must not interfere with the work of other users or the performance of School systems and networks.
- Staff must not access, create, store, download, share or transmit content that is illegal, discriminatory, obscene, hateful, extremist, offensive or otherwise inappropriate.

- Staff must not attempt to bypass, disable or interfere with the School's filtering, monitoring or security systems.
- Staff should exercise professional judgement when accessing information online and should be mindful of the accuracy, reliability and suitability of digital content.
- Staff must respect copyright and intellectual property rights and must not upload, download, copy or distribute copyrighted material without appropriate permission or lawful authority.
- Staff should be aware that activity undertaken using School devices, systems and networks may be monitored and recorded in accordance with the School's safeguarding, security and legal responsibilities. Misuse of School systems or technology may result in disciplinary action and, where appropriate, referral to external agencies.

Use of Personal Devices

Within this policy, the term *personal device* refers to any portable equipment capable of connecting to the internet, storing or transmitting data, capturing images, recording audio or video, or supporting digital communication.

This includes, but is not limited to:

- Mobile phones
- Laptops
- Tablets
- Smartwatches and other wearable technology
- Cameras
- Audio or video recording devices
- Any other internet-enabled, data-enabled or image-capturing device
- Staff may use personal devices during non-contact time, such as breaks and lunch periods, when they are not responsible for supervising pupils. Personal devices should not be used for personal reasons in the presence of pupils during the school day. Limited professional use is permitted where required for safeguarding, communication, educational or operational purposes.
- Staff may use the personal Wi-Fi access provided by the School to connect personal devices to the wireless network, but access credentials must not be shared with others.
- Any personal device used to access School systems or data must be protected by an appropriate password, passcode or biometric security measure. Lost or stolen devices with access to School systems must be reported immediately to the ICT Team.
- Staff must not use personal devices to capture, store, process or share photographic or video imagery of pupils or pupil personal data except in the exceptional circumstances outlined within the School's Online Safety and Digital Awareness Policy and Staff Code of Conduct.
- Staff from all sections of the School must not use personal devices at any time whilst in proximity to pupils from Bradshaw.
- Personal mobile phones, cameras and other electronic devices with imaging or sharing capabilities belonging to staff working with EYFS children, or other staff who are in contact with them (including catering staff), must be stored out of sight and must not be used in their presence. This applies not only within the EYFS building but also whenever staff are working with or supervising EYFS children in any location.
- Staff may wear smartwatches provided they do not have photographic capabilities. Emerging technologies such as smart glasses or other wearable devices with image, audio or video recording functionality must not be worn or used in the presence of EYFS children.

Use of Digital Photographic and Video Imagery

- Staff must only use School-approved equipment and systems when capturing, storing, sharing or publishing photographic or video imagery of pupils.
- Staff must ensure that pupils are aware when imagery is being taken wherever reasonably practicable and that imagery is captured in a manner that protects the dignity, wellbeing and privacy of pupils.
- All imagery must be transferred to and stored on School-approved systems and shared only through authorised School communication channels or agreed internal processes.

- Staff must respect parental preferences regarding the publication of pupil images and ensure that imagery is used in accordance with the School's safeguarding, data protection and publication procedures.

In Exceptional Circumstances

Only with the express permission of the Head or Deputy Head (Pastoral) may staff use a personal device to capture photographic or video imagery of pupils.

Where such authorisation is granted:

- The use must be appropriate, necessary and consistent with safeguarding requirements.
- The imagery must be intended solely for approved School purposes.
- Pupils should be aware that imagery is being taken wherever reasonably practicable.
- The device must be secured appropriately.
- The imagery must be transferred to a School-approved system as soon as reasonably practicable.
- The imagery must be deleted from the personal device immediately following transfer.
- The imagery must not be shared through personal accounts, devices, applications or communication channels.

Commissioned Photographers and External Providers

Staff responsible for commissioning photographers or other external providers must ensure that:

- Images are captured only for the agreed purpose.
- Pupils are aware that imagery is being taken.
- Imagery is stored and transferred securely.
- Parental permissions are respected.
- Images are used in accordance with the School's safeguarding, data protection and publication procedures.

Use of Technology with Pupils

Staff should actively supervise and support pupils when using technology and should take reasonable steps to ensure that digital resources, websites and online services are suitable for the age and needs of the pupils involved.

Where pupils are permitted to search the internet independently, staff should provide appropriate supervision and guide pupils towards safe, reliable and age-appropriate sources of information wherever possible.

Staff should reinforce online safety messages and good digital practices whenever technology is used with pupils, ensuring that:

- Pupils understand the purpose and expectations of the Pupil Acceptable Use Policy (AUP) and are encouraged to use technology safely, responsibly and respectfully, both in and out of school.
- Pupils are taught to think critically about the information they encounter online and to evaluate the reliability, accuracy and suitability of digital content.
- Pupils are encouraged to acknowledge sources appropriately and to respect copyright and intellectual property when using digital materials.
- Pupils are supported in understanding online risks, including cyberbullying, online scams, misinformation, inappropriate content, artificial intelligence (AI) and the importance of protecting personal information.

Artificial Intelligence (AI)

- Staff must use artificial intelligence (AI) tools responsibly and in accordance with the School's safeguarding, data protection, confidentiality and professional conduct requirements.
- Staff remain responsible for all content created, edited, reviewed or shared using AI tools.
- Personal, confidential or sensitive information relating to pupils, parents, staff or the School must not be entered into AI systems unless authorised and compliant with the School's data protection requirements.

- AI-generated content must be reviewed for accuracy, appropriateness and safeguarding considerations before use.
- AI must not be used to create, manipulate or share misleading, deceptive, harmful or inappropriate content relating to pupils, staff or the wider school community.

Use of Online Communications

Within this policy, the term *online communication* refers to any platform that enables users to communicate, collaborate, create, publish or share content. This includes, but is not limited to, email, messaging services, social media platforms, online forums, blogs, gaming platforms, livestreaming services and other digital communication tools.

Staff should consider carefully, before posting, sharing or responding to content online, the potential impact on their own professional reputation, the reputation of others and the reputation of the School.

Staff must ensure that their online behaviour reflects the same professional standards expected within the workplace and is consistent with the values of The Winchester House Way.

Staff must not make comments or share content that is inappropriate, offensive, discriminatory, defamatory, unlawful, misleading or likely to damage the reputation of individuals or the School.

Staff must not engage in cyberbullying, harassment, intimidation or any other online behaviour that could cause harm to another person.

Staff should be mindful that information shared online may be copied, stored, distributed or viewed beyond its intended audience and may remain accessible indefinitely.

Staff must not interact with current pupils through personal social media accounts, messaging services or other personal online platforms.

Staff should exercise professional judgement when interacting online with former pupils and must ensure that any communication remains appropriate, professional and consistent with the Staff Code of Conduct.

Any communication with pupils should take place through School-approved systems and communication channels.

Reporting Procedures

Staff must ensure that any safeguarding concern relating to the use of technology by pupils, staff or any other member of the School community is reported immediately to the appropriate Designated Safeguarding Lead (DSL) in accordance with the School's safeguarding procedures.

Staff must ensure that any concern relating to the misuse of School equipment, systems, networks or digital technologies, including any suspected illegal activity, is reported immediately to the Group Director of ICT and the appropriate Designated Safeguarding Lead.

Staff must ensure that any concern regarding inappropriate, harmful or potentially illegal content being accessible through School systems or networks is reported immediately to the Group Director of ICT and the appropriate Designated Safeguarding Lead.

Staff must report any suspected security breach, unauthorised access, loss of School data or other incident that may affect the security of School systems, information or users.

Agreement

Please complete the section below to confirm that you have read, understood and agree to follow the principles contained within the Staff Acceptable Use Policy.

Failure to comply with this policy may result in access to School devices, systems or networks being withdrawn and may lead to disciplinary action in accordance with School procedures.

Name of Staff Member:

Signed:

Date: