Horris Hill School

Digital & Technology Acceptable Use Policy

Date of review: July 2025

Date of publication: September 2025

Date of next review: September 2026

Person(s) responsible for review and role:

Head of School - Helen Wilkinson

Head of Lower School and Nursery – Laura Wowk

Assistant Director of Education: Alex Brough

Aim of policy:

The purpose of this policy is to outline the acceptable use of technology in the school, this includes the use of any internet access, school owned devices, pupil owned devices, mobile phones and any other technology used on the school premises and whilst under the care of school staff such as on trips, fixtures and visits. It also applies to the use of technology off School premises whilst in the care of the school, where the culture or reputation of the School or any member of its community are put at risk.

Related Guidance and School Policies

This policy outlines the acceptable use of technology but is not exhaustive in its scope and should be used in conjunction with the following policies, statutory guidance and advice:

- *Equivalent of safeguarding and child protection policy*
- *Good Behaviour and Sanctions Policy*
- *Anti-Bullying Policy*
- *RSE and PSHEE policy*
- *Pupil code of conduct*
- *Early Years Framework*
- *KCSIE 2025*
- Preventing and Tackling Bullying (DfE July 2017)
- Sharing nudes and semi nudes: advice for education settings (UKCIS updated March2024)
- Relationships education, relationships and sex education and health education guidance (DfE September 2025)
- Searching, screening and confiscation: advice for schools (DfE July 2022)
- Teaching online safety in school (DfE Jan 2023)
- Online Safety Act (2023)

Use of Technology

The school makes use of a variety of methods to include technology within the curriculum, in all cases the rationale for its use first takes consideration to the safeguarding of the pupils and the material they can access. Consideration is then given to how the technology supports the delivery of the curriculum and how to avoid the use of the technology replacing the desired outcomes of the learning.

Digital skills and literacy are essential though it is important that pupils are equally given the knowledge and skills to utilise technology appropriately. The School will support pupils to develop their understanding at an age appropriate level that includes restricting access to the internet to balance the safety and welfare of pupils, the security of our technology systems, and access to resources required by the curriculum. The school utilises filtering systems through Lightspeed to provide reports and alerts of any inappropriate use on school devices or whilst using the school infrastructure to access the internet.

All pupils receive a school account with a school email address. This account should be used when accessing any school resources or systems and not shared with others. Those applications, websites or other software that require a login for school related work should use the assigned school account and not transfer any data, images, recordings, or other information to personal storage, email or other systems. Pupils are not permitted to install or remove any applications or other software from school owned or issued devices, doing so may be considered a serious breach of discipline.

Pupils are required to sign and acknowledge that they have read this policy and the appropriate acceptable use policy as can be found in this policy. Pupils should sign the prep school acceptable use policy.

Pupils should be aware that the school makes use of filtering and monitoring systems, through Lightspeed. These systems allow the school to identify pupils where inappropriate behaviour has been detected, on school owned or

issued devices this may also then include the system taking a screen shot of the content or search, make use of keylogging to give contextual understanding to the behaviour before the incident in addition to retaining the internet browsing history on the device.

In the case of boarding pupils this also applies to any internet access whilst in the boarding house made on devices. Using devices for non-academic purposes whilst in the boarding house is permitted however this must not contravene the boarding code of conduct, school code of conduct or the boarding acceptable use policy, of which all boarding pupils are required to have read and signed. Pupils in the boarding house should also consider the impact that technology and screens can have on the quality of sleep they have, where possible blue light filters or night modes should be used an technology should be put away ideally at least an hour before lights out.

Whilst the School recommends that parents only give their child technology to reflect their emotional maturity, the use of applications and software that is rated at an age appropriate level beyond the child's age are not permitted to be used on the school premises, or whilst the pupil is under the care of school staff, including in the boarding house and on school trips and visits.

Pupils are not permitted to have a mobile phone in school.

If in any case a pupil's device can access the internet outside of the School Wi-Fi network then parents must ensure that their child's own device has appropriate filtering software installed (to filter access via 3G,4G, 5G or GPRS). Where appropriate or required, all devices should have parental security enabled with 'safe searching'. Additionally, where pupils bring their own device, such as phone, laptops and tablets, parents should ensure that appropriate anti-malware software is installed and that this is kept up to date. The school takes no responsibility for any personal devices and they are brought to school at the pupils own risk.

Acceptable Use for Pupils

All pupils are responsible for their actions when using technology. Pupils should never share any login credentials to their accounts with others. Use of technology should be safe, responsible, respectful to others and in accordance with the law. If a pupil is aware of misuse by other pupils or if a pupil is worried about something they have seen on the internet, or on any electronic device, including another person's electronic device, they should talk to a teacher about it as soon as possible.

Any misuse of technology and/or breach of this policy will be dealt with in accordance with the behaviour policy, and pupil code of conduct. However, incidents involving the misuse of technology which are considered to be of a safeguarding and/or bullying nature will be dealt with in accordance with the School's Safeguarding and Child Protection Policy and/or the Anti-Bullying Policy and procedures as appropriate.

If a pupil thinks that they might have been bullied or that another person is being bullied, they should talk to a teacher as soon as possible. See the School's Anti-Bullying Policy for information about cyberbullying, bullying associated with prejudice and/or discrimination and e-safety.

Unacceptable use of technology may result in the School restricting access to School IT systems and internet use, a cancellation of a pupil's email account, refusal of permission to use personal devices on the School premises or while in the care of the School. Confiscation of devices and/or material may be deleted and/or disciplinary action may be taken. If there are reasonable grounds to suspect that the confiscated device contains evidence in relation to an offence such as sharing nudes or semi-nude pictures and/or videos or upskirting, or that it contains pornographic material of an extreme nature or of a child, the device will be given to the police.

Rules for photographs, videos and images

You may only use school owned devices to take images or recording of school related activities or make or generate content in relation to the school. This includes the use of artificial intelligence to generate content, text, images or videos. The only exception to this would be the capture of images specifically for the use within the photography non-examined assessment, research and enrichment activities. In such cases you must have the permission of a member of staff and those involved in the image. Any such images or recording may only be used expressly for the purpose of the enrichment activity as outlined by the member of staff or as directed in conjunction with the guidance outlined by the relevant examination board and associated body for accreditation, in the case of those eligible for access to public examination funds this will commonly be the joint council for qualifications (JCQ).

The posting of images which may be deemed by the School to be offensive, or which brings the School into disrepute, can be considered a serious breach of discipline and in such cases will be subject to disciplinary procedures irrespective of whether the image was posted using School or personal device/s.

Searching of pupil owned devices

Using material of any kind to bully, harass, discriminate, or intimidate others will constitute may constitute a serious breach of discipline. Should staff have sufficient concern to need to search a pupil owned device the procedure below will be followed. In all cases this should be only done in order to establish if the concern is upheld and the extent thereof. Staff should be specific and only ask to see applications or content relating to the concern. Staff should never ask for personal passwords, pin codes or similar credentials from pupils to access content at a later date. Additionally staff should follow safeguarding practices. If content of an offensive, disturbing, pornographic or criminal nature is found then the device will be confiscated.

- Permission will be sought from the headteacher in which the extent of the concern will be outlined
- The pupil will then be asked to show the member of staff their device, the pupil must hold the device in a manner that ensures the screen is visible to the staff member at all times. The staff member will then ask the pupil to show them content from a specified time period or where this is unknown may ask the pupil to scroll through the images or messages on the device from applications, websites or software that specifically relate to the concern raised. Where a pupil refuses to comply with such a request, should the concern be of a sufficient nature the police may be contacted directly at this point. Where this is not necessary the pupil may be subject to disciplinary procedures.
- If any images are of an extreme pornographic nature or a pornographic image of a child, or is a still or moving image that has been obtained by ‘upskirting’ this will not be deleted and the device will be confiscated and delivered to the police rather than asked to show any suspected content. This also applies for material that may be considered to be of a radical nature.
- Should content be found that would be considered concerning to the welfare of the pupil or other pupils then appropriate safeguarding concerns and referrals should be made.
- In the event content that supports the concern and/or that requires the device to be confiscated is found then parents will be informed. If no content is found and the device does not require confiscation parents will be contacted to explain the reason for the original concern and further support may be offered as there are likely to be wider contextual issues.

Pupils should be aware that the sharing of nudes and semi-nudes, whether or not you are in the care of the School at the time the image is recorded and/or shared may constitute a criminal offence even if the picture is taken and shared with the permission of the person in the image. The School will treat incidences of sharing nudes and semi-nudes (both sending and receiving) as a serious breach of discipline and also as a safeguarding matter under the School’s Child Protection procedures.

Pupils should remember that the earlier they report an issue the more can be done to limit the extent to which it is shared or distributed. Particularly in relation to content shared or posted to social media. If you are concerned about

any image you have received, sent, or forwarded or otherwise seen, speak to any member of staff for advice. If sexual images or videos have been made or circulated online, the Internet Watch Foundation may be able to assist with their removal.

Searching of school owned devices and accounts

The School has the right to access the contents of a School Issued Device or account at any time, pupils emails are subject to monitoring at any time and the school retains ownership of any content, images, recordings and data produced and stored using school systems. Any breach of this policy or related policies in relation to school owned devices may be considered a serious breach of discipline.

Acceptable Use Policies

Pupils are required to read this policy and the appropriate acceptable use policies for their age or attendance at particular activities for the school. Copies of these can be found on the subsequent pages.

Artificial Intelligence

When using AI to generate content pupils should not:

1. Claim authorship of material that is generated by AI in addition to appropriately referencing any material they use within their work generated by AI.
2. Use AI to generate source code for academic work.
3. Use AI to generate spam, malicious communications or other malicious software.
4. Use AI to attempt to bypass or otherwise deliberately avoid the monitoring and filtering systems in place.
5. Use AI to generate content that would be considered offensive including but not limited to nudity, obscene gestures and material that would be considered radical.
6. Use AI to generate political material or propaganda.
7. Use AI to implement fully automated decision making for academic related work.

Senior School Acceptable Use Policy
Academic Year 2025/2026

School devices and systems are strictly for schoolwork. By following these rules and guidelines, you help maintain a safe and productive learning environment for everyone at our school. These rules and guidelines also apply should you bring your own personal device to school.

Internet Access

1. The school monitors internet and technology use through both filtering and monitoring systems. The school utilises Lightspeed to achieve the filtering of content at an age-appropriate level in addition to providing monitoring reports to the pastoral team where inappropriate use has been detected.
2. The school's Wi-Fi or network should not be used for social media or instant messaging. Follow the current procedures for network access and do not use personal email accounts through the school's network.
3. Do not bypass security facilities, anti-virus software, or internet filtering systems; doing so may result in suspension of internet access may be considered a serious breach of discipline.
4. Understand that not everything on the internet is accurate, you should look to gain information from multiple credible sources and always speak to a member of staff if you are unsure.
5. Do not open email attachments from unknown senders; delete such attachments immediately and report them to your teacher.

Conduct

1. Secure individual codes and passwords must be used for all devices and accounts; do not share them with others. You are responsible for your accounts and devices. Do not deliberately access, send, or share offensive or illegal material. Report accidental encounters with such material or inappropriate sites to a staff member immediately.
2. Only use your school email address to contact staff; do not communicate with staff via social networking sites unless it's a school trip phone number during a school trip or visit (which must be removed after the trip). These devices and numbers are owned by the school and are not personal contact details for staff.
3. Do not use technology to bully, intimidate, or radicalize others; this is a serious breach of discipline even if it occurs outside of school.
4. Understand that technology use can be addictive, use blue light filters where possible and reflect on the amount of time you spend both on active and passive screen time each day.

Devices

1. No device is allowed in examination rooms unless approved by the invigilator and as part of an agreed access arrangement made in advance with approval of the examination board.
2. Images or recordings made on school premises require staff permission and must be used only for school purposes; do not distribute them outside the school's network or upload them to social media. Such images or recordings should only be made using school owned devices with permission from those involved.
3. Screens in classrooms must only be used with a staff member present and with explicit permission.
4. Use school owned devices only for learning activities and educational purposes.
5. Take care with school owned devices and any data; avoid damage to the device or loss through carelessness or leaving it unattended.
6. You should only sign up for approved sites or apps where given permission to do so by a member of staff.
7. Report broken or lost school owned devices to your teacher as soon as possible
8. Understand that school owned devices may be subject to remote monitoring by the school at any time.
9. Mobile phones are not permitted in school and must be handed into the designated point at the start of the school day should you bring one. The school takes no responsibility should this be lost, stolen or damaged.

Software

1. Do not download or install any software or programs onto school technology.
2. Do not attempt to hack or damage any software, computer systems, networks, or IT equipment. This may be considered a serious breach of discipline.

Artificial Intelligence in Education

1. Use artificial intelligence (AI) tools responsibly and only for educational purposes. AI should enhance learning and not replace your own efforts.
2. Do not use AI to complete assignments or exams dishonestly. Always ensure that the work you submit is your own.
3. Understand the limitations of AI and verify the information it provides. AI can assist with research but should not be the sole source of information.
4. Be aware of the ethical implications of AI use, including privacy concerns and data security. Use AI tools that comply with school policies and data protection regulations.

Importance of Plagiarism

1. Plagiarism is the act of using someone else's work or ideas without proper attribution. It is a serious academic offense.
2. Always credit the original authors when using their work. This includes direct quotes, paraphrased ideas, and any material such as images that are not your own.
3. Use proper citation methods as instructed by your teachers. This helps maintain academic integrity and respect for intellectual property.
4. Understand that plagiarism can have severe consequences, including disciplinary action.

I have read and understood the above points and agree to follow the rules and guidelines. I understand that failure to adhere to the standards or the school’s policies may result in a serious breach of discipline.

Name: .....

Form: .....

Signature: .....

Date: _ _ / _ _ / _ _ _ _

Preparatory School Acceptable Use Policy
Academic Year 2025/2026

School devices and systems are strictly for schoolwork. By following these rules and guidelines, you help maintain a safe and productive learning environment for everyone at our school. These rules and guidelines also apply should you bring your own personal device to school.

Internet Access

1. The school checks your use of the internet and technology use through both filtering and monitoring systems. The school uses Lightspeed to do this so you can see content at an age-appropriate level. It also gives monitoring reports to the pastoral team where inappropriate use has been detected.
2. The school's Wi-Fi or network should not be used for social media or instant messaging. Follow the current process for network access and do not use personal email accounts through the school's network.
3. Do not try to get around security facilities, anti-virus software, or internet filtering systems; doing so may result in suspension of internet access may be considered a serious breach of discipline.
4. Understand that not everything on the internet is accurate, you should look to gain information from multiple credible sources and always speak to a member of staff if you are unsure.
5. Do not open email attachments from unknown senders; delete such attachments immediately and report them to your teacher.

Conduct

1. Secure individual codes and passwords must be used for all devices and accounts; do not share them with others. You are responsible for your accounts and devices. Do not deliberately access, send, or share offensive or illegal material. Report accidental encounters with such material or inappropriate sites to a staff member immediately.
2. Only use your school email address to contact staff; do not communicate with staff via social networking sites unless it's a school trip phone number during a school trip or visit (which must be removed after the trip). These devices and numbers are owned by the school and are not personal contact details for staff.
3. Do not use technology to bully, intimidate, or radicalize others; this is a serious breach of discipline even if it occurs outside of school.
4. Understand that technology use can be addictive, use blue light filters where possible and reflect on the amount of time you spend both on active and passive screen time each day.

Devices

1. Images or recordings made on the school site require staff permission and must be used only for school purposes; do not share them outside the school's network or upload them to social media. Such images or recordings should only be made using school owned devices with permission from those involved.
2. Screens in classrooms must only be used with a staff member present and with explicit permission.
3. Use school owned devices only for learning activities and educational purposes.
4. Take care with school owned devices and any data; avoid damage to the device or loss through carelessness or leaving it unattended.
5. You should only sign up for approved sites or apps where given permission to do so by a member of staff.
6. If you choose to bring your own device to school daily it should be adequately charged and in a suitable case. You should access the schools Wi-Fi using the instructions you are given.
7. Report broken or lost school owned devices to your teacher as soon as possible
8. Understand that school owned devices may be subject to remote monitoring by the school at any time.

9. Mobile phones are not permitted in school and must be handed into the designated point at the start of the school day should you bring one. The school takes no responsibility should this be lost, stolen or damaged.

Software

1. Do not download or install any software or programs onto school technology.
2. Do not attempt to hack or damage any software, computer systems, networks, or IT equipment. This may be considered a serious breach of discipline.

Artificial Intelligence in Education

1. Use artificial intelligence (AI) tools responsibly and only for educational purposes. AI should enhance learning and not replace your own efforts.
2. Do not use AI to complete assignments or exams dishonestly. Always ensure that the work you submit is your own.
3. Understand the limitations of AI and verify the information it provides. AI can assist with research but should not be the sole source of information.
4. Be aware of the ethical implications of AI use, including privacy concerns and data security. Use AI tools that comply with school policies and data protection regulations.

Importance of Plagiarism

1. Plagiarism is the act of using someone else's work or ideas without stating where it has come from. It is a serious academic offense.
2. Always credit the original authors when using their work. This includes direct quotes, paraphrased ideas, and any material such as images that are not your own.
3. Use the referencing methods as instructed by your teachers. This helps maintain academic integrity.
4. Understand that plagiarism can have severe consequences, including disciplinary action.

I have read and understood the above points and agree to follow the rules and guidelines. I understand that failure to adhere to the standards or the school's policies may result in a serious breach of discipline.

Name: .....

Form: .....

Signature: .....

Date: _ _ / _ _ / _ _ _ _

Boarding Acceptable Use Policy
Academic Year 2024/2025

School devices and systems are strictly for schoolwork. By following these rules and guidelines, you help maintain a safe and productive learning environment for everyone at our school. These rules and guidelines also apply should you bring your own personal device to school.

Internet Access

1. The school monitors internet and technology use through both filtering and monitoring systems. The school utilises Lightspeed to achieve the filtering of content at an age-appropriate level in addition to providing monitoring reports to the pastoral team where inappropriate use has been detected.
2. The school's Wi-Fi or network should not be used for social media or instant messaging. Follow the current procedures for network access.
3. Do not bypass security facilities, anti-virus software, or internet filtering systems; doing so may result in suspension of internet access may be considered a serious breach of discipline.

4. Understand that not everything on the internet is accurate, you should look to gain information from multiple credible sources and always speak to a member of staff if you are unsure.
5. Do not open email attachments from unknown senders; delete such attachments immediately and report them to your teacher.
6. Boarders may access a wider range of recreational and entertainment sites through the schools Wi-Fi though the same rules of conduct apply. Pupils should not attempt to access or view content that is not age appropriate for all who can view it.

Conduct

1. Secure codes and passwords must be used for all devices and accounts; do not share them with others. You are responsible for your accounts and devices. Do not deliberately access, send, or share offensive or illegal material. Report accidental encounters with such material or inappropriate sites to a staff member immediately.
2. Only use your school email address to contact staff; do not communicate with staff via social networking sites unless it's a school trip phone number during a school trip or visit (which must be removed after the trip). These devices and numbers are owned by the school and are not personal contact details for staff.
3. Do not use technology to bully, intimidate, or radicalize others; this is a serious breach of discipline even if it occurs outside of school.
4. Understand that technology use can be addictive, use blue light filters where possible and reflect on the amount of time you spend both on active and passive screen time each day.
5. Devices should be turned off and mobile phones handed in before lights out in the evening, mobile phones cannot be taken into the main school site during the main school hours.

Devices

1. Images or recordings made on school premises require staff permission and must be used only for school purposes; do not distribute them outside the school's network or upload them to social media. Such images or recordings should only be made using school owned devices with permission from those involved.
2. Take care with school owned devices and any data; avoid damage to the device or loss through carelessness or leaving it unattended.
3. You should only sign up for approved sites or apps where given permission to do so by a member of staff.
4. Report broken or lost school owned devices to your teacher as soon as possible
5. Understand that school owned devices may be subject to remote monitoring by the school at any time.

Software

1. Do not download or install any software or programs onto school technology.
2. Personal boarding devices must have appropriate antiviral software installed and where they can access materials online without the school Wi-Fi they must have age appropriate parental controls and filtering in place.
3. Do not attempt to hack or damage any software, computer systems, networks, or IT equipment. This may be considered a serious breach of discipline.

Artificial Intelligence

1. Use artificial intelligence (AI) tools responsibly and only for educational purposes. AI should enhance learning and not replace your own efforts.
2. Be aware of the ethical implications of AI use, including privacy concerns and data security. Use AI tools that comply with school policies and data protection regulations.

I have read and understood the above points and agree to follow the rules and guidelines. I understand that failure to adhere to the standards or the school's policies may result in a serious breach of discipline.

Name: .....

Form: .....

Signature: .....

Date: _ _ / _ _ / _ _ _ _