

WHOLE SCHOOL ACCEPTABLE USE OF TECHNOLOGY PROCEDURE FOR STUDENTS

Please also refer to the Early Years Mobile Phone and Camera procedure

1 Scope

This procedure is addressed to all students, and parents are encouraged to read it with their child. A copy of the policy is available to parents on request, and the School actively promotes the participation of parents to help the School safeguard the welfare of students and promote the safe use of technology.

The School will take a wide and purposeful approach to considering what falls within the meaning of technology. This procedure relates to all technology, computing and communications devices, network hardware and software and services and applications associated with them, including but not limited to:

- the internet
- email
- mobile phones and smartphones
- desktops, laptops, netbooks, tablets
- personal music players
- devices with the capability of recording and/or storing still or moving images
- social networking and blogging
- instant messaging (including image and video messaging via apps such as Snapchat and WhatsApp), chat rooms, blogs and message boards
- webcams, video hosting sites (such as YouTube)
- gaming sites
- Virtual Learning Environments such as Firefly and Teams
- SMART boards
- other photographic or electronic equipment e.g. GoPro devices and drones
- the use of AI platforms e.g. ChatGPT
- any device capable of capturing or sharing images

This procedure applies to the use of technology on School premises.

This procedure also applies to the use of technology off School premises if the use involves students or any member of the School community, or where the culture or reputation of the School are put at risk. Additional rules on the use of technology in boarding houses are provided in the Boarders' Handbook.

Related policies and procedures

- *Behaviour Policy*
- *Whole School Anti-Bullying Policy including Anti-Cyber Bullying*
- *Online Safety Policy*
- *Safeguarding and Child Protection Policy*

2 Aims

The aims of this procedure are:

- to educate and encourage students to make good use of the educational opportunities presented by access to technology
- to safeguard and promote the welfare of students, in particular by anticipating and preventing the risks arising from:
 - exposure to harmful or inappropriate material (such as pornographic, radicalising, extremist, racist, or offensive materials) the sharing of personal data, including images, videos, and sounds;
 - the sharing of personal data, including images, videos, and sounds
 - inappropriate online contact or conduct
 - cyberbullying and other forms of abuse
- to minimise the risk of harm to the assets and reputation of the School
- to help students take responsibility for their own safe use of technology (i.e. limiting the risks to which children and young people are exposed when using technology)
- to ensure that students use technology safely and securely and are aware of both external and peer to peer risks when using technology
- to prevent the unnecessary criminalisation of students

3 Safe use of technology

We want students to enjoy using technology and to become knowledgeable users of online resources and media. We recognise that this is crucial for further education and careers.

The School will support students to develop their skills and make internet access as unrestricted as possible, whilst balancing the safety and welfare of students and the security of our systems.

1.1 Online safety and emerging technologies

Students should understand that online safety forms part of the School's safeguarding responsibilities and that risks can arise from the use of technology both within and outside of School.

Students should be aware that online risks may arise through:

- content they see online, including harmful, misleading, extremist, violent or age-inappropriate material
- contact from unknown individuals or those seeking to exploit, manipulate or groom children
- conduct online, including bullying, harassment, intimidation, image sharing, hate incidents and other harmful behaviour
- commerce-related risks, including scams, fraud, gambling and misleading advertising

Students should exercise critical thinking when viewing online content and recognise that information, images, videos and audio may be inaccurate, manipulated, artificially generated or deliberately misleading.

Students are educated about the importance of safe and responsible use of technology to help them to protect themselves and others online.

Students may find the following resources helpful in keeping themselves safe online:

<https://www.thinkuknow.co.uk/>

<https://www.childnet.com/>

<https://www.childline.org.uk/Pages/Home.aspx>

<https://www.ceop.police.uk/safety-centre/>

Please see the whole School *ICT Across the Curriculum Policy* for further information about the School's teaching of ICT.

4 Internet and email

The School provides internet access and an email system to support students' academic progress and development.

All students will receive guidance on the use of the School's internet and email systems. The New Hall School email account is provided to Senior Divisions students primarily to enable students to communicate with other members of the school community in an appropriate manner. If students are unsure about what constitutes appropriate use, they must seek assistance from a member of staff. The New Hall School email account is provided to Preparatory Divisions parents and pupils solely to enable access to Firefly and other School approved remote learning platforms.

For the protection of all students, all incoming and outgoing electronic data will be monitored for inappropriate content by the School. Students should remember that even when electronic data has been downloaded and deleted, it can still be traced on the system. Students should not assume that files stored on servers or storage media are private.

Microsoft Teams

Microsoft Teams provides communication tools that teaching staff may use for remote learning opportunities. Students should follow the guidelines below when using Microsoft Teams.

When using Microsoft Teams, remember that this is an extension of the classroom and you should conduct yourself as you would in a classroom. You should:

- use Microsoft Teams in an environment that is quiet, safe and free from distractions
- make sure that you are on time for your virtual learning sessions
- dress appropriately for learning
- ensure that your mobile phone is switched off during sessions to avoid distractions and interruptions
- close off other applications and focus fully on the session
- always interact patiently, positively and respectfully with your teachers and peers
- start every session with your microphone on mute until the teacher asks you a direct question

5 School rules

Students **must** comply with the rules and principles outlined in Appendix 1 (Senior Divisions) and Appendix 2 (Preparatory Divisions), which all students will be required to adhere to.

The purpose of these rules is to set out the principles which students must follow at all times to use technology safely and securely.

These principles and rules apply to all uses of technology.

6 Use of mobile phones

The School's expectation is that students do not have access to mobile phones during the School day. This is in line with current statutory government guidance. This approach is intended to promote learning, wellbeing, positive social interaction, and safeguarding. Students must either leave their mobile phone at home or hand it in on arrival at School to the Student Reception. A student who is found carrying, using or concealing a mobile phone during the School day will receive a sanction in accordance with the School's *Behaviour Policy*, and the device will be confiscated in line with School procedures. Persistent breaches will be treated as a more serious disciplinary matter.

Students who require a mobile phone, or other electronic device, for the monitoring or management of a medical condition (for examples, diabetes monitoring) may be permitted to retain and use their device in accordance with their agreed medical or healthcare plan, and any arrangements approved by the School.

7 Procedures

Students are responsible for their actions, conduct and behaviour when using technology at all times. Use of technology should be legal, safe, responsible and respectful to others. If students are aware of misuse by other students, they should report it to a member of staff as soon as possible.

Any misuse of technology by students will be dealt with under the School's *Behaviour Policy*.

Students must not use technology to bully others. Bullying incidents involving the use of technology will be dealt with under the School's *Anti-Bullying Policy including Anti-Cyber Bullying*. If students think that they have been bullied, or that another person is being bullied, they should report it to a member of staff as soon as possible.

In any cases giving rise to safeguarding concerns, the matter will be dealt with under the School's child protection procedures (see the School's *Safeguarding & Child Protection Policy*). If students are worried about something that they have seen on the internet, or on any electronic device, including on another person's electronic device, they must report it to a member of staff as soon as possible.

In a case where students are considered vulnerable to radicalisation, they may be referred to the Channel programme. Channel is a programme which focuses on providing support at an early stage to people who are identified as being vulnerable to being drawn into terrorism.

In addition to following the procedures in the relevant policies as set out above, all serious incidents involving technology must be reported to the Designated Safeguarding Lead and the IT Manager who will record the matter centrally.

8 Sanctions

Where a student breaches any of the School rules, practices or procedures set out in this procedure or the appendices, the relevant Head of Division will apply any sanction which is appropriate and proportionate to the breach, in accordance with the School's Behaviour Policy, including, in the most serious cases, expulsion. Other sanctions might include; increased monitoring procedures, withdrawal of the right to access the School's internet and email facilities and/or detention. Any action taken will depend on the seriousness of the offence.

Unacceptable use of electronic devices or the discovery of inappropriate data or files could lead to confiscation of the device or deletion of the material in accordance with our policies and procedures.

The School reserves the right to charge students or their parents for any costs incurred by the School as a result of a breach of this procedure.

9 Monitoring and review

All serious safety incidents involving technology will be logged centrally by the Lead Designated Safeguarding Lead and the IT Manager. The IT Manager is responsible for the effective operation of the School's network. They monitor the use of technology as set out in this procedure and maintain the appropriate logs.

Consideration of the effectiveness of the School's e-safety procedures and the education of students about keeping safe online will be included in the annual review of safeguarding for Governors.

ACCEPTABLE USE OF TECHNOLOGY AGREEMENT

The School has the responsibility of providing you with safe, reliable and useful ICT resources that will help you to make the most of your learning opportunities. The School also allows you to bring your own mobile devices onto School premises. With these rights, however, come the following responsibilities:

1 Access and security

- a) I understand that access to the internet from the School's devices and network is for educational purposes only.
- b) I understand that the School cannot guarantee the confidentiality of content created, shared and exchanged via School systems. I will ensure that my online communications, and any content shared online, are respectful of others and composed in a way I would wish to stand by.
- c) I understand that I must not use the School's facilities or network for personal, social or non-educational use without the express prior consent of a member of staff.
- d) I will not knowingly obtain (or attempt to obtain) unauthorised access to any part of the School's or any other computer system, or any information contained on such a system.
- e) I understand that passwords protect the School's network and computer system. I will not let anyone else know my password. If I believe that someone knows my password, I will change it immediately.
- f) I will not attempt to gain unauthorised access to anyone else's computer or to confidential information which I am not authorised to access. If there is a problem with my passwords, I will speak to my class teacher or contact the ICT support staff.
- g) I will not attempt to access or share information about others without the permission of a member of staff. To do so may breach data protection legislation and laws relating to confidentiality.
- h) I am aware that the School has cybersecurity in place to ensure the safety and security of the School's networks. I will not attempt to disable, defeat or circumvent any of the School's cybersecurity facilities. I will report any problems to a class teacher or the IT Support Team.
- i) I am aware that the School has filtering systems in place to block access to unsuitable material, wherever possible, to protect the welfare and safety of students. I will not try to bypass this filter.
- j) I will not load material from any external storage device brought in from outside the School onto the School's systems, unless this has been authorised by the IT Manager.

- k) I am aware that viruses can cause serious harm to the security of the School's network and that of others. Viruses are often spread through internet downloads or circulated as attachments to emails. If I think or suspect that an attachment, or other downloadable material, might contain a virus, I will report it to IT Support before opening the attachment or downloading the material.
- l) I will not disable or uninstall any anti-virus software on the School's computers.
- m) I am responsible for ensuring that all requested operating system updates are performed on my school tablet. These will help provide important security patches, which will help to keep me and my data safe online.
- n) I understand that it is an expectation that school tablets have Bluetooth turned on at all times, as this will enable staff to monitor my safe use of online resources and applications.
- o) I will not attempt to add applications to any device without the express consent of the IT Manager. I am aware that requests for educational applications are welcome using the online form on Firefly.
- p) I understand that methods for overcoming limitations placed on a school device such as 'jailbreaking' are treated with the utmost seriousness.

10 Use of the internet

- a) I will take care to protect personal and confidential information about myself and others when using the internet, even if information is obtained inadvertently. I will not put personal information about myself, for example my full name, address, date of birth or mobile number, online.
- b) I will assume that all material on the internet is protected by copyright and such material must be treated appropriately and in accordance with the owner's rights. I will not copy or plagiarise another's work.
- c) I will not view, retrieve, download or share any offensive material. Offensive material includes, but is not limited to, content that is abusive, racist, considered to be of an extreme or terrorist-related nature, sexist, homophobic, bullying, pornographic, defamatory or criminal in nature. I am aware that use of technology in this way is a serious breach of discipline and may constitute a serious criminal offence. I will tell a member of staff immediately if I have accidentally read, downloaded or have been sent any offensive material or material that is inappropriate, including personal information about someone else.
- d) I understand that not all information online is accurate and trustworthy.
- e) I will consider the reliability of online sources and seek guidance where I am unsure whether information, images, videos, or audio are genuine.

- f) I understand that misinformation and disinformation can cause harm and I will not knowingly create or share false or misleading content.
- g) I will not communicate with staff using social networking sites or other internet or web-based communication channels unless this is expressly permitted for educational reasons.
- h) I will not bring the School into disrepute through my use of the internet.

11 Use of email

- a) I understand that the School's email system is intended to support students in their academic progress and development. I know that all communications should be appropriate. I understand that examples of inappropriate communications are those, which are abusive, racist, terrorist-related, sexist, homophobic, bullying, pornographic, defamatory or criminal, in nature. I will not send or forward trivial messages or jokes through the School's email system. I understand that not only could these cause distress to recipients (if considered to be inappropriate), but could also cause the School's network to suffer delays and/or damage.
- b) I understand that all correspondence from my School email account will contain the School's disclaimer.
- c) I will not read anyone else's emails without their consent.

12 Use of mobile electronic devices
--

- a) I understand that 'mobile electronic device' includes but is not limited to mobile phones, smartphones, smart watches, smart glasses, ,mobile electronic devices.
- b) I understand that mobile phones and other personal devices can present safeguarding risks, including exposure to harmful content, cyberbullying, inappropriate contact, online grooming, image-based abuse, scams and misinformation.
- c) I understand that students in Years 7-11 are not permitted to use their mobile phones, smartphones or smart watches whilst on the School site (this includes break and lunchtimes).
- d) I understand that mobile phones, and smart watches must be either left at home, or handed in to Student Reception during the School day.
- e) I understand that students who have approval to use a mobile phone or electronic device for the monitoring or management of a medical condition may retain and use that device in accordance with their agreed healthcare arrangements.
- f) I understand that if a student in Years 7-11 is seen using a mobile or smartphone during the normal academic School day, they will be escorted to reception to hand it in and will receive a Yellow Card. If, however, the student needs the device for safe travel home, then this can be collected at the end of the School day from student reception but must be returned to student reception no later than 8.45am the following school day.

- g) I understand that for Sixth Form students, mobile or smartphones are permitted only in the Sixth Form area.
- h) I understand that the use of smart phones during the School day should not be necessary. In emergencies, I may request to use the School telephone. Should my parents wish to contact me in an emergency, they should telephone the School Reception and a message will be relayed promptly.
- i) I will not communicate with staff using a mobile phone (or other mobile electronic device), except when this is expressly permitted by a member of staff, for example when necessary during an educational visit. I understand that any such permitted communications should be brief and courteous.
- j) I understand that use of mobile electronic devices of any kind to bully, harass, intimidate or attempt to radicalise others will not be tolerated and will constitute a serious breach of discipline, whether or not I am in the care of the School at the time of such use. Appropriate disciplinary action will be taken where the School becomes aware of such use.
- k) I understand that mobile electronic devices may be confiscated and searched in appropriate circumstances.
- l) I understand that all mobile electronic devices are brought into School at my own risk. I understand that all devices should require a passcode or password to be unlocked and this should never be divulged to any other student.
- m) I understand that the School does not accept any responsibility for the theft, loss of, or damage to, mobile electronic devices brought onto School premises, including devices that have been confiscated or which have been handed in to staff, and I am aware that the school insurance does not cover the loss of mobile electronic devices.

13 Photographs and images

- a) I understand that using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.
- b) I understand that no photograph should be taken of any other student without their express permission.
- c) I will only use cameras or any mobile electronic device to take a still or moving image with the express permission of the member of staff in charge and with the permission of those appearing in the image.
- d) I will allow staff access to images stored on mobile phones, cameras or devices and must delete images, if requested to do so.
- e) I understand that the posting of images which are considered to be offensive or which bring the School into disrepute is a serious breach of discipline and that students implicated in such behaviour will be subject to disciplinary procedures.

- f) Shared nude, semi-nude or intimate images: I will not create, request, possess, store, share or distribute nude, semi-nude or intimate images or videos of any child or young person. I understand that this includes digitally altered, manipulated or AI-generated images. I understand that doing so may constitute a criminal offence. If I commit such an act, it is likely that the local statutory authorities will be consulted and a School disciplinary sanction will be applied. Local statutory authorities include the Police Service and the Essex Safeguarding Children Board, although this list is not exhaustive.
- g) I understand that if I receive such material, I should not forward, save or share it and should report it immediately to a member of staff.
- h) I understand that once a photograph or message is sent, I have no control over how it is passed on. I may delete the image, but it could have been saved or copied and may be shared by others.
- i) I understand that images shared online become public and may never be completely removed. They could be found in the future by anyone, even by universities and future employers.
- j) If I am concerned about any image I have received, sent or forwarded or otherwise seen, I will speak to any member of staff for advice.

6 Use of Artificial Intelligence (AI)
--

- a) I understand that AI tools, including generative AI platforms, must only be used in accordance with staff instructions and for legitimate educational purposes.
- b) I will not use AI tools to produce work that I submit as entirely my own where this has not been authorised by my teacher.
- c) I understand that AI-generated information may be inaccurate, misleading, biased or incomplete and should always be checked against reliable sources.
- d) I will not use AI tools to create, share, manipulate or distribute images, audio, video or text that could cause harm, embarrassment, harassment or distress to another person.
- e) I understand that creating or sharing AI-generated intimate images, altered photographs or so-called 'deepfakes' of another person may constitute a serious safeguarding concern and may result in disciplinary action and referral to external agencies where appropriate.

Student name:

Tutor Group:

Student signature:

Date:

ACCEPTABLE USE OF TECHNOLOGY AGREEMENT (PREPARATORY DIVISIONS)

This agreement should be read by pupils in the Preparatory Division with their parents. When the agreement is shared via Parentmail, parents are asked to confirm their child understands the agreement. In the Pre-Prep Division, parents are asked to confirm they understand the agreement on behalf of their child.

The School has the responsibility of providing you with safe, reliable and useful ICT resources that will help you to make the most of your learning opportunities. The School also allows boarders and those travelling on School transport to bring their own mobile devices onto School premises. With these rights however, come the following responsibilities:

a) Access and security

I understand that I should access the internet from School devices and network for educational purposes only.

I understand that I must not use the School devices and network for personal, social or non-educational use without permission from a member of staff.

I understand that passwords protect me and also protect the School. I will not let anyone else know my password. If I believe that someone knows my password, I will change it immediately or tell a member of staff.

I will not use anyone else's login or password.

I understand that the School uses filtering and monitoring systems to help keep students safe online.

I understand that my activity on School networks, systems and devices may be monitored for safeguarding, security, and operational purposes.

I will not attempt to bypass, disable, or interfere with any filtering, monitoring or safeguarding systems.

I will not share information about other people without permission from a member of staff.

I will not use any external storage device (e.g. a memory stick) brought in from outside the School, unless with express permission from a member of staff.

b) Use of the internet

I will not put personal information about myself or anyone else online, for example my full name, address, date of birth or mobile number.

I will not try to view, download or share any inappropriate material. I will tell a member of staff immediately if I think I have accidentally seen, read or downloaded material that is inappropriate. I will also minimise the window on a desktop computer, close a laptop lid or close an iPad case so that others do not also see the material.

I understand that not all information online is accurate and trustworthy.

I will consider the reliability of online sources and seek guidance where I am unsure whether information, images, videos, or audio are genuine.

I understand that misinformation and disinformation can cause harm and I will not knowingly create or share false or misleading content.

I will not try to communicate with a member of staff using social networking sites or other internet or web-based communication channels, other than when instructed to do so on School-approved systems.

I will not bring the School into disrepute through my use of the internet.

c) Use of email

I understand that the School's email system is intended to support students in their academic progress and development.

d) Use of mobile electronic devices
--

I understand that 'mobile electronic device' includes but is not limited to mobile phones, smartphones, smart watches, tablets, laptops and MP3/MP4 players.

I understand that mobile phones and other personal devices can present safeguarding risks, including exposure to harmful content, cyberbullying, inappropriate contact, online grooming, image-based abuse, scams and misinformation.

I understand that if I have brought a mobile electronic device into School because I travel on School transport, it is to be handed in to reception when I arrive and collected when I depart.

I understand that use of mobile electronic devices of any kind to bully, harass, intimidate or attempt to radicalise others will not be tolerated and will constitute a serious breach of discipline, whether or not I am in the care of the School at the time of such use. Appropriate disciplinary action will be taken where the School becomes aware of such use.

I understand that mobile electronic devices may be confiscated and searched in appropriate circumstances.

I understand that all mobile electronic devices are brought into School at my own risk. I understand that all devices should require a passcode or password to be unlocked and this should never be divulged to any other student.

I understand that the School does not accept any responsibility for the theft, loss of, or damage to, mobile electronic devices brought onto School premises, including devices that have been confiscated or which have been handed in to staff, and I am aware that the school insurance does not cover the loss of mobile electronic devices.

e) Photographs and images

I understand that using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.

I understand that no photograph should be taken of any other pupil without their express permission.

I will only use cameras or any mobile electronic device to take a still or moving image with express permission from the member of staff in charge and with the permission of those appearing in the image.

I will allow staff access to images stored on mobile phones, cameras or devices and must delete images if requested to do so.

I understand that the posting of images which are considered to be offensive or which bring the School into disrepute is a serious breach of discipline and will be subject to disciplinary procedures.

I will not send indecent images of myself or others. I understand that this can be against the law. If I commit such an act, it is likely that the local statutory authorities, including the Police, will be consulted and a school disciplinary sanction will be applied.

I understand that once a photograph or message is sent, I have no control over how it is passed on. I may delete the image, but it could have been saved or copied and may be shared by others.

If I am concerned about any image I have received, sent or forwarded or otherwise seen, I will speak to any member of staff for advice.

7 Use of Artificial Intelligence (AI)
--

f) I understand that AI tools, including generative AI platforms, must only be used in accordance with staff instructions and for legitimate educational purposes.

g) I will not use AI tools to produce work that I submit as entirely my own where this has not been authorised by my teacher.

h) I understand that AI-generated information may be inaccurate, misleading, biased or incomplete and should always be checked against reliable sources.

i) I will not use AI tools to create, share, manipulate or distribute images, audio, video or text that could cause harm, embarrassment, harassment or distress to another person.

- j) I understand that creating or sharing AI-generated intimate images, altered photographs or so-called 'deepfakes' of another person may constitute a serious safeguarding concern and may result in disciplinary action and referral to external agencies where appropriate.