HOLMWOOD HOUSE
SCHOOL

Information Technology (IT)
Acceptable Use Policy for pupils

The School encourages all parents to read through this with their children. All pupils must agree to the contract in Appendix 1, which is in their prep diaries, at the start of each academic year.

1. Principles

1.1 We are committed to ensuring your safety and that of our staff at all times, as well as the preservation of our reputation locally, nationally and internationally.

1.2 We want you to keep abreast of change within the world of electronic and real-time media communication and are aware of and appreciate the power of IT when used appropriately for educational purposes.

1.3 We will support you in becoming empowered and responsible digital creators and users.

1.4 We will support you to be kind online and want you to help us to create a school community that is respectful and caring, on and offline; and for you to be safe and be sensible online and always know that there is someone to talk to.

1.5 The supply of school managed devices, the network and internet access is intended to enhance the educational and working environment for its users.

1.6 The objective of this policy is to outline to you the terms and conditions of use governing the use of school managed devices, the use of personal devices on the school wifi, use of the school network and any internet access. All users are expected to abide by the policy in its entirety.

1.7 This policy sets out social media guidelines and online safety advice for you.

2. Definitions and clarifications

2.1 Any electronic, mobile, computing device used within the school, whether connected to the network or not (for example laptops, tablets and mobile phones [Year 7 & 8 boarders only]) including those not owned by Holmwood House but connected to the network, whether wirelessly, cabled or otherwise will be referred to as a ‘device’.

2.2 ‘School managed devices’ are those managed by the school IT technician such as chromebooks, networked computers, mobile phones and tablets.

2.3 Any device used for storing data where files can be posted, including but not limited to USB memory sticks, memory cards, CD/DVD/Blu-Ray discs, external hard drives, and any online sites will be referred to as a ‘site or storage device’.

2.4 ‘Cloud services’ are systems such as Google Suite or other school managed online services.

2.5 Any communication application, websites, platforms or other app used for text messaging, posting messages, will be referred to as ‘social media platforms’.

2.6 Cyber- Bullying is the use of IT, particularly mobile phones or social media platforms on the internet, deliberately to upset someone else.

2.7 You should be aware that this policy is also applicable when connecting to any external network outside of the Holmwood House system (including ISPs) whilst at Holmwood House or in the care of Holmwood House.

2.8 The DSL is the School’s Designated Safeguarding Lead, the Deputy Head.

2.9 In cases where clarification may be required regarding the contravention of any principles in this policy, the Headteacher and/or DSL have the ultimate say.

3. Monitoring

3.1 In line with the Education Act 2011, Keeping Children Safe in Education (September 2021), Searching, screening and confiscation (January 2018), and other Department for Education guidelines, the School reserves the right to monitor your use of the Internet, confiscate and search any devices e.g. mobile phones or chromebooks where there is reason to suspect a pupil's safety is endangered or non-compliance with this policy.

3.2 You must understand that the information you access using the school network, held on the school network or cloud services or accessed via school managed devices is not private and may be inspected.

3.3 You must also understand that the School reserves the right to check your emails or social media platforms which you have visited using school or personal devices whether at home or in school (where you have used your school account or school device). This is especially important where your welfare or that of another individual is believed to be endangered.

3.4 Automated reports are generated by our filtering systems showing all internet access and e-mail activity using the school network (allowed and blocked) whether on school managed devices or personal devices (using your school account or school device) which are routinely reviewed by the DSL.

3.5 The use of Blocklisted Apps on school-managed devices is monitored and will be reported to the Deputy Head and consequences will follow as stated in Section 4.

4. Consequences

4.1 Actions which are considered to contravene this or other school policies and which can be traced to a pupil may be subject to disciplinary action under the School's Anti Bullying Policy and/or the Behaviour Policy. The specific sanction imposed will depend on the seriousness of the incident and will be more severe for repeated offences.

4.2 Misuse of a School Chromebook that contravenes item 10.5 below will result in at least a Show Down but the Heads of Phase and/or Deputy Head may use more severe sanctions (as per the Sanctions pyramid) for repeated or serious offences.

4.3 Pupils who attempt to access material contrary to this policy might have their access to WIFI removed.

4.4 Support and counselling may be put in place for those developing addictive tendencies.

4.5 Given that failure to adhere to these regulations can have a seriously detrimental effect on the individual/s involved, and the reputation of the school, it should be recognised that a pupil may face permanent exclusion and that this serious punishment can be applied even for a first occurrence and irrespective of the pupil's school record.

4.6 The School reserves the right to report, where appropriate, infringements of these regulations to the Police or other agencies, as a variety of criminal offences (such as harassment, abuse, racism, slander, character defamation) may fall within the definitions of the legal offences.

5. Online Safety

5.1 Personal Safety: You need to be aware that you may jeopardise your personal safety either at School or outside School through online communication or by email. You should therefore:

- Take care in responding to emails requesting personal details or that contain links.
- Be aware that any person you "meet" or communicate with online may pretend to be someone else.
- Never arrange a meeting in person with anyone they have "met" or only communicated with online.
- Not respond to messages or bulletin board items that are indecent, suggestive, belligerent, discriminatory, threatening, or which make you feel uncomfortable or unsafe in any way.
- Remember that anything you read online may not be accurate.
- Ignore offers that involve either financial transactions or personal meetings.

- Not disclose any personal details, such as your home address or telephone number, across the Internet.

5.2 You should report any concerns to your Head of Phase, the IT technician regarding cyber-security or the DSL regarding online safety.

6. Cyber-Bullying

6.1 Cyber-Bullying is just another method of bullying; for further information and sanctions please see the School's Anti Bullying Policy. This sets out the particular dangers of Cyber-Bullying.
6.2 Examples of Cyber-Bullying behaviour include (not exhaustive):

- Setting up website pages and inviting others to post derogatory comments about a pupil.
- Filming incidents and circulating the film clips via mobile phones or on-line.
- Sending insulting or vicious messages by messaging platforms including the spreading of malicious rumours about another pupil/pupils.
- Posting fake and obscene photographs [known as nudes or semi-nudes] of another pupil on messaging platforms.
- Hacking into messaging platforms and removing and circulating material which may be embarrassing or personal.
- Hijacking and changing the details on someone's messaging platform when they leave it open and vulnerable OR setting up fake profile sites to impersonate and insult someone via a social media or messaging platform

6.3 If you or another pupil is the victim of Cyber-Bullying, you should: inform your Head of Phase and/or tutor, or another member of staff about this as soon as possible; and preserve evidence, e.g. texts, messages, e-mails or images, rather than delete them.
6.4 You will be held responsible for all material that you place on social media platforms and for any material that is placed on social media platforms where you are the account holder.
6.5 Misconduct of this type carried out during the holidays or when you are out of School remains subject to School discipline if the welfare of other pupils or the culture and reputation of the School are placed at risk.
6.6 Action and sanctions may include confiscation of devices, restrictions on the use of the Internet or network, and the contacting of other agencies such as the police.

7. Email and online communication

7.1 The School acknowledges your rights to use email and online communication including social media platforms, such as WhatsApp or Google Meets. The School encourages the use of social media platforms and acknowledges their place in increasing opportunities to learn and in promoting positive, respectful and thought-provoking discussions.
7.2 The School has high standards and expectations for appropriate online and email communication.
7.3 You should be aware when using school email that your name may appear next to any information posted and could be linked back to you.
7.4 Words and images posted on to email could be shared widely by being forwarded to many other people and if you choose to write emails you should consider this.

7.5 To safeguard all of our pupils, employees and the reputation of the school, the following conditions should be adhered to by Holmwood House pupils when using social media or on email:

- Users must refrain from writing or posting any comments that are disrespectful to individuals, or are obscene [rude], inappropriate, inflammatory [cause someone to have angry feelings] or defamatory [damaging the reputation] towards the school or any part of it.
- Holmwood House expects that online discussions you or any pupils participate in are polite and non-offensive.

7.6 There is a catch-all offence under Section 127 of the Communications Act 2003. This makes it illegal to send "by means of a public electronic communications network a message that is grossly offensive or of an indecent, obscene or menacing character". You must not:

- Put yourself into a position where anything posted might bring Holmwood House into disrepute.
- Represent your own personal views as those of Holmwood House on any social media sites.
- Write or post anything that could be considered disrespectful, insulting, threatening, harassing, inappropriate, illegal, inflammatory (makes people feel angry), abusive, rude, sexual, damages someone's reputation, false, or aggressive towards any individual or Holmwood House.
- Be discourteous and refrain from using any impolite, indecent, abusive, discriminatory, racist or abusive language in emails.
- Discuss or post personal information about other pupils or members of staff at Holmwood House, including phone numbers, email addresses or any confidential information.
- Post any material that compromises the rights of any Holmwood House pupil, or member of staff of Holmwood House, including privacy, intellectual property, or publication rights.
- Allow any other individual to use your identification for posting or viewing comments.
- Post comments under multiple names or using another person's name.
- Nothing should be written on email or posted onto websites or messaging platforms that could be considered as victimising and or humiliating someone on account of their gender, race, religion, nationality, culture, disability or sexual orientation. Please see the School's Equal Opportunities Policy for more information.
- Staff are not allowed to have current pupils as 'friends' on any personal social media account and are discouraged from having recent former pupils as friends.

8. Use of the internet and cloud services

8.1 The School is required to do all that they reasonably can to limit pupils' exposure to the risks online using appropriate filters and monitoring systems.

8.2 There are three areas of risk that the School monitors:

- Content: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views.
- Contact: being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults.
- Conduct: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

8.3 You are encouraged to use the Internet. We regard the use of the Internet to search for information related to a school subject or to a recreational hobby as acceptable. You are expected to sign annually to acknowledge you have read the Acceptable Use of IT guidance in your prep diary.

8.4 You must not:

- Disclose to a third party the personal details of any other individual.
- Breach another person's copyright in any material.

- Upload or download any unauthorised software or attempt to run that software. In particular hacking, encryption and other system tools are expressly forbidden.
- Use the computer network to gain unauthorised access to any other computer network.
- Introduce a VPN without the consent of the Director of Digital Learning
- Attempt to spread computer viruses.
- Engage in activities that are prohibited under UK Law. Thus the transmission of material subject to copyright or protected by trade secret is forbidden.

8.5 Encrypted information flowing through the school network and internet connection including, but not limited to, e-mails, cloud services, and web site access can be decrypted by our systems in order to properly inspect data for security and filtering purposes. Where for technical reasons a service cannot be decrypted access to this service may be blocked. Decryption will not be performed on services categorised as sensitive, for example banking and medical.

9. Legal issues

9.1 Staff members and pupils should be aware that laws relating to libel, defamation, harassment and copyright may apply to information posted online on social media platforms, including:

- Libel Act 1843
- Defamation Acts 1952 and 1996
- Protection from Harassment Act 1997
- Criminal Justice and Public Order Act 1994
- Malicious Communications Act 1998
- Communications Act 2003, and
- Copyright, Designs and Patents Act 1988.

10. Network and devices

10.1 Disciplinary action will be taken against those found to be in breach of the terms and conditions outlined that follow. Failure to comply will result in reference to the School's Senior Leadership Team.

10.2 When serious breaches of the terms and conditions have occurred parents of pupils will be informed by either the Deputy Head, and where relevant be treated as a safeguarding matter and referred to the police.

10.3 The main points of this policy can be summarised into the nine key sentences below. No users are permitted to undertake any of the following actions:

- Logging on to the school network or cloud services with another user's account.
- Using computers to send offensive or harassing material to others.
- Altering the settings of the computers or making other changes which render them unusable by others.
- Tampering physically with the equipment.
- Installing software on school computers.
- Hacking into unauthorised areas of the network.
- Accessing inappropriate websites or trying to get around the school's systems. This includes the use of VPNs or proxy servers for this purpose.
- Using computers while at school for any form of illegal activity.

10.4 General conduct and use of the network and devices:

- Pupils should always show consideration for other users, e.g. volume at which items are listened to or the way the computer is left.
- Any damage to, or theft of, computers, furniture or fitments should be reported to a member staff without delay. The same applies to any equipment which seems to not be working.
- Pupils must not use the system in such a way as to disrupt the use of the network, cloud services or work stations by other users.
- Pupils must respect this facility and avoid damaging computers, computer systems or networks. Furthermore, if anyone discovers any methods of causing such damage he/she must report them to the relevant member of staff.

- Before leaving a device, pupils must always log off the network and check that the logging out procedure is complete.
- When logging on to the network pupils must always use their own user identification and password. Pupils must understand that any attempt to impersonate another individual or systems administrator will be treated as a serious offence, as will any attempt to interfere with data stored on the network by another user.
- Any pupil who identifies a security problem on the Holmwood House network or cloud services must notify their teacher immediately.
- Pupils must never give their passwords to other users or to people outside the school. Any pupil who suspects that their password has been compromised, accidentally or otherwise, should change their password without delay and inform the IT technician. If an act is committed using another individual's login details then that individual must expect to be punished as if they had committed the act. It is therefore very important that you keep your login details secure.

- Pupils must not attempt to gain access to the local drive of any machine or to create local accounts (administrative or otherwise).
- All Holmwood House installed software is subject to change and may be updated or removed at the school's discretion when deemed necessary.
- Only software that has been provided on the network may be run on the computers. Pupils are not permitted to import or download applications or games onto shared machines.
- It is the responsibility of a device's owner to ensure that they have a licence for any additionally installed software over and above that which is already provided with a device.

- The School cannot accept responsibility for any damage, howsoever caused, to personal devices or their contents (files, folders etc.).

- Pupils must be aware of, and comply with, the restrictions placed on certain kinds of usage; notably the playing of games on machines, where others wish to do academic work.

- Pupils must understand that under no circumstances should computers, printers or other devices be detached from the network to make way for personal devices.
- No servers, switches, hubs or routers of any description should be attached to the network.
- Connecting privately owned wireless access points to any part of the network is strictly forbidden unless permission has been granted by the IT technician.

10.5 The use of School Chromebooks

- Chromebooks will be confiscated and examined if it is considered they are being used in contravention of any aspect of this Policy
- It is your responsibility to ensure your Chromebook is working at all times. You should contact the IT technician if there is an issue.
- You must bring your Chromebook to lessons every day with sufficient charge.
- Chromebook may only be used in lessons and classrooms with the express permission of your teachers. Only content or apps that are relevant to the lesson should be accessed. Chromebook should be closed at all other times.
- If you lose your Chromebook you must inform IT immediately in order that they can consider what personal information may have been lost or is at risk of being lost.
- Your Chromebook must remain in your possession, should only be used by you and should be securely stored when not in use.
- Your Chromebook must be clearly labelled with your name and remain in its protective case at all times when you are not using it.
- Backup of content on the Chromebook (e.g. to Google Drive) is your responsibility.
- We reserve the right to ask for the removal of any Blocklisted app or app or that is counter to the principles of this policy and as yet un-Blocklisted (principles in 8.2).
- The use of your Chromebook functions such as the camera function is forbidden unless authorised by a teacher or for clear educational purposes.

Useful websites

The following websites provide information, guidance and practical advice on issues related to social media and online safety

- https://nationalonlinesafety.com/
- http://www.saferinternet.org.uk/
- www.thinkuknow.co.uk
- https://www.internetmatters.org/
- http://www.childnet.com/
- www.childline.org.
- https://www.gov.uk/government/publications/preventing-and-tackling-bullying
- https://www.disrespectnobody.co.uk/sexting/what-is-sexting/
- https://www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation

Written and reviewed by ERLB & FCB October 2021

Appendix 1

Pupil Contract – to be signed in prep diaries at the start of each academic year.

When using school chromebooks/computers:

Do:

- Only use chromebooks/computers at school when you have permission
- Only use your school google account (including your email) for school work
- Only ever use your own ID and password
- Always keep your password secret
- Always log off when you are finished
- Always be polite and considerate in emails and digital communication
- Always handle school chromebooks and computers with care and respect
- Report any faults to your teacher straight away
- Report any inappropriate material that you accidentally come across to your teacher
- Report any cyberbullying to a teacher

Never:

- Never log on using another person’s details
- Never give away your password
- Never attempt to alter any computer settings
- Never access other people’s files, unless shared with you
- Never deliberately seek out inappropriate material
- Never attempt to bypass the school’s safety filters
- Never access games sites unless directed to do so, by a teacher
- Never attempt to download/upload to your school account any programs/files/extensions unless you have permission from the Head of ICT

- Never publish personal details about yourself or anyone that you know, online

Acceptable Use Agreement:

- I agree to abide by these rules when using school equipment or my school google login
- I understand that the the school monitors my files and account, including internet pages I visit and emails, for my safety
- I understand that misbehaviour using my school account may result in restrictions or a ban being applied

Signed: