Haileybury
International Summer School

Haileybury International Summer School
E-Safety Policy

Policy date:	April 2024
Date of next review:	April 2025
Owner:	Summer School Director
Intended audience:	Summer School Pupils, Parents, Staff
Location:	Summer School Website and Summer School Staff Handbook

1. Scope and purpose

1.1 Haileybury International Summer School ('Summer School') aims to provide a first-class experience for its pupils, including having time and access to facilities for recreation and relaxation after lessons. On desktops located in the academic areas of the Summer School, pupils must use the internet appropriately (e.g. no playing games/shopping online etc.).

1.2 We know access to technology is vital to enable pupils to maintain contact with family and friends while away from home. However, pupils need to have adequate and quality sleep to learn effectively, and thus they should not be making video calls, web searching or using social networks late into the night. For this reason, wi-fi access in boarding houses via the Summer School network is suspended between 10 pm and 7 am each day.

1.3 It is important to teach pupils how to stay safe in the e-environment and how to avoid making themselves vulnerable to a range of risks, including identity theft, bullying, harassment, grooming, stalking and abuse. There will be an orientation session covering online safety whilst at Summer School both in the house meeting and in class.

2. Role of our IT Department

2.1 With the explosion in the use of technology, the Summer School recognises that blocking and barring sites is no longer adequate on its own, although filters are in place on the Summer School network. The Summer School needs to ensure that pupils understand why they need to behave responsibly if they are to protect themselves.

2.2 The Summer School's technical staff have a key role in maintaining a safe technical infrastructure at the Summer School and keeping abreast of the rapid succession of technical developments. They are responsible for the security of the Summer School's hardware system, its data and training its teaching and administrative staff to use ICT. They monitor the use of the internet and emails and report inappropriate usage to the Summer School Director, Chief Operating Officer and also the Designated Safeguarding Lead (DSL) and team.

2.3 The Summer School recognises that internet safety is a child protection and general safeguarding issue. The Summer School DSL holds responsibility for safety issues involved with the misuse of the internet and other mobile electronic devices. As part of their induction training, Summer School and the Safeguarding Team have received Online Safety training and guidance in e-safety issues.

2.4 Users must accept that the Summer School has access to all files; a file may be accessed to read a pupil's work, check for abusive/unacceptable material or for possible damage to the system (e.g. viruses).

2.5 Users accept that their time spent on the Summer School network is monitored by the Summer School, either directly, remotely, or both. This is to ensure the safety of pupils and that the network is being used for the intended purpose.

2.6 In exceptional circumstances, emails may be read on the instructions of the Summer School Director.

3. Internet and email

3.1 Use of the internet is a privilege, not a right. In the event of abuse, access will be removed. Pupils are provided with a Summer School email account; use of web-based mail (Hotmail/Yahoo etc.) is not allowed.

4. Social media

4.1 Snapchat, Instagram and Tik Tok all have a minimum age of 13. WhatsApp's minimum age is 16. We understand that apps on pupils' devices apps cannot be regulated or removed by the Summer School. However, staff members will not encourage the use of these apps. Should it come to the attention of Summer School staff that pupils are using apps with age limits under these ages, we will get in contact with the pupils' parents to advise them of this and recommended that they are deleted. Any negative behaviour associated with these apps, such as bullying, will be dealt with as a separate behaviour issue, and it will be recommended that they delete the app. Summer School staff members will not access pupils' devices to delete apps at any time. At induction, pupils will be made aware of the UK age restrictions on these apps, and it will be recommended that they pause their use of the apps during the Summer School or risk sanctions.

5. Misuse: Statement of Policy

5.1 The Summer School will not tolerate any illegal material such as downloading and sharing audio, video and DVD files, either internally or from the internet, which is a breach of copyright laws and therefore illegal, except from legitimate pay sites. The Summer School will always report illegal activity to the Police.

5.2 If the Summer School discovers that a pupil is at risk because of online activity, it may seek assistance from the Child Exploitation and Online Protection Unit (CEOP). The Summer School Director will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with the Summer School's *Behaviour, Discipline and Exclusions Policy*.

6. Charter for the safe use of the internet and electronic devices at the Summer School

6.1 E-safety is a whole Summer School responsibility, and at the Summer School the staff and pupils have adopted the following charter for the safe use of the internet inside the Summer School:

Cyberbullying

- Cyberbullying is a particularly harmful form of bullying because it can be so pervasive and anonymous. There can be no safe haven for the victim who can be targeted at any time or place. The Summer School's *Behaviour, Discipline and Exclusions Policy* describes the preventative measures and the procedures that will be followed when the Summer School discovers cases of bullying.
- Pupils are prohibited from sending ‘spoof’ emails to recipients.
- Proper supervision of pupils plays an important part in creating a safe ICT environment at Summer School, but everyone needs to learn how to stay safe outside the Summer School.
- The Summer School values all its pupils equally. It is part of the Summer School's ethos to promote considerate behaviour and to value diversity.
- Bullying and harassment in any form should always be reported to a member of staff. It is never the victim's fault, and he or she should not be afraid to come forward.

Treating other users with respect

- The Summer School expects pupils to treat staff and each other online with the same standards of consideration and good manners as they would during face-to-face contact.

- The Summer School expects a degree of formality in communications between staff and pupils and would not normally expect them to communicate with each other by text or mobile phones. On educational visits, when communication by mobile phone may be appropriate, staff members never give out their personal mobile numbers or social media details to pupils.
- Pupil mobile numbers are held centrally with the Admin Officer/Summer School Director who will provide those details to staff on trips should they need to contact the pupil.
- Everyone has a right to feel secure and to be treated with respect, particularly the vulnerable. Harassment and bullying will not be tolerated, and this is set out in the Summer School’s Behaviour, Discipline and Exclusions Policy. The Summer School is strongly committed to promoting equal opportunities for all, regardless of race, gender, gender orientation or physical disability.
- All pupils are encouraged to look after each other and report any concerns about the misuse of technology or worrying issues to a staff member.
- The use of cameras on mobile phones in washing and changing areas are not allowed.

Build a positive online reputation

- Pupils should consider the long-term impact of what they post online. Future employers and universities are likely to conduct online searches of prospective employees/ pupils. Remember that if you post something linked to your name, your reputation could be damaged or enhanced accordingly.
- Pupils should also check their privacy settings on social media.

Not bringing the Summer School into disrepute

- Pupils must not use the logo, other branding, or the name of "Haileybury International Summer School" on social media or websites without specific permission having first been obtained from the Summer School Director. Pupils must not bring the good name of the Summer School into disrepute by their actions, online messages, or posts.

Keeping the Summer School network safe

- The Summer School adheres to best practices regarding e-teaching and the internet.
- The Summer School's filtering system blocks certain sites, and the Summer School's IT Department monitors pupils' use of the network. Pupils must not attempt to circumnavigate these filters by other means, e.g. using proxy servers or VPNs.
- The IT Department monitors email traffic and blocks spam and certain attachments.
- The Summer School issues all pupils with their own Haileybury Summer School email address. Access is via a personal login, which is password protected. The Summer School gives guidance on the reasons for always logging off and for keeping all passwords securely.
- The network must not be used for commercial purposes or unauthorised advertising.
- The Summer School has strong anti-virus protection on its network, which the IT Department operates.
- Any member of staff or pupil who wishes to connect a removable device to the Summer School's network is asked to arrange in advance with the IT Department to check it for viruses and ensure its compatibility.

Safe use of personal electronic equipment

- The Summer School's guidance is that pupils and staff should always think carefully before posting any information online and be careful to log off/lock their computers when working in public areas. Pupils are not permitted to access others accounts/information or files or to misuse the network.
- Content posted should not be deemed inappropriate, offensive or likely to cause embarrassment to the individual or others. Posts could also impact on the reputation of individuals and the wider Summer School community. Pupils should not bring the good name of the Summer School into disrepute since they will be in breach of our rules and face sanctions.
- The Summer School offers guidance on the safe use of social networking sites and cyberbullying in orientation sessions, which covers blocking and removing contacts from 'friend lists'.
- The Summer School's orientation sessions include guidance on how pupils can identify the signs of a cyber-stalker and what they should do if they are worried about being harassed or stalked online.
- The Summer School offers guidance on keeping names, addresses, passwords, mobile phone numbers and other personal details safe. Privacy is essential in the e-world.
- The Summer School advises on the responsible use of Skype and appreciates that free video calls can provide pupils with an invaluable means of maintaining contact with their families and friends.

Considerate use of electronic equipment

- Mobile phones, smartphones, iPods and other personal electronic devices should be switched off and stored in the pupils’ lockable space during the day. They may be used during break times. However, mobiles should be switched off during lessons and activities etc.
- Staff may confiscate personal equipment that is being misused during the Summer School day until the end of the lesson or the end of the day. If a password-protected electronic device is confiscated due to suspicious usage in breach of this E-Safety Policy, pupils must be willing to share passwords to enable investigation of any alleged offences. Failure to share such passwords is likely to mean that further serious disciplinary action will follow.
- Sanctions may be imposed on pupils who tamper with/damage hardware or use their electronic equipment without consideration for others.

The Summer School expects all pupils to adhere to this charter for the safe use of the internet. Use of the Summer School network by pupils depends on their compliance with this Policy on acceptable use; an audit may be carried out at any time to ensure compliance. Any misuse may result in disciplinary action.

7. Involvement with parents and guardians

7.1 The Summer School will always contact parents if it has any concerns about pupils' behaviour in this area, and likewise, it hopes that parents will feel able to share any concerns with the Summer School.

8. Data protection, privacy and monitoring

8.1 The Summer School has appointed the Chief Operating Officer as the Data Protection Officer, who can be contacted if you have any concerns with data protection at dataprotection@haileybury.com. For more information, please visit the Summer School website, which contains the Summer School's Child Friendly Privacy Statement.

8.2 The Summer School monitors the usage of its network to ensure compliance with legislation in force from time to time. Examples include:

- Data Protection Act 2018.
- General Data Protection Regulation 2018.
- Sexual Offences Act 2003.
- Human Rights Act 1998 and the European Convention of Human Rights (if applicable).
- Interception of Communications Act 1995.
- Video Recordings Act 1984.

9. Disclaimer

1. The Summer School is not responsible for the quality, accuracy or content of any material accessed from any networks or originating from sources not directly managed by the Summer School or its staff.
2. The Summer School is not responsible for the quality, accuracy or content of any materials that an individual user may make available within or outside the Summer School through the network.
3. The Summer School is not responsible for the provision of internet services that are supplied by a third party. However, the Summer School will make every effort to ensure continuity of service.
4. Despite the Summer School investing in considerable improvements to its internet service, wi-fi coverage and available bandwidth over the past few years, it cannot guarantee bandwidth to pupil users at any given time.
5. While being prepared to make reasonable adjustments where possible, the Summer School does not guarantee that all devices (e.g. Windows phones & Kindles) will be fully compatible with its systems.
6. The Summer School does not undertake to repair pupils' own computer equipment, such as personal laptops. It might be possible to assist pupils in getting their equipment repaired by third parties, but the Summer School does not offer any guarantee in terms of those services or repairs.
7. Given the Summer School's rural location, pupils should note that both mobile signal coverage and strength of mobile signal are beyond our control.

Version history		
Date	**Reviewed by**	**Notes**
August 2021	Summer School Director	New policy
April 2024	Summer School Director and Commercial Operations Director	Reviewed