Cobham Hall

POLICY STATEMENT ON DIGITAL COMMUNICATIONS

In the modern world technology is a crucial component of every academic subject and is also taught as a subject in its own right. Several of the school's classrooms are equipped with electronic whiteboards and all have projectors and computers. Cobham Hall has three ICT suites in the school and students may use the machines there and in the ILC for private study. All of the school's boarding houses are equipped with computers and network points and Wi-Fi access points.

All students at Cobham Hall are taught how to research on the internet and to evaluate sources. They are educated into the importance of evaluating the intellectual integrity of different websites and why some apparently authoritative sites need to be treated with caution. Some free, online encyclopaedias do not evaluate or screen the material posted on them.

THE ROLE OF TECHNOLOGY IN OUR STUDENTS' LIVES

Technology plays an enormously important part in the lives of all young people. Smart devices that are internet enabled provide unlimited access to the internet, IM messaging, blogging, social media, Skype, wikis (collaborative web pages), chat rooms and video sharing sites.

This communications revolution gives young people unrivalled opportunities. It also brings risks. It is an important part of the school's role to teach students how to stay safe in this environment and how to avoid making themselves vulnerable to a range of risks, including identity theft, bullying, harassment, grooming, stalking and abuse. They also need to learn how to avoid the risk of exposing themselves to subsequent embarrassment. The school reserves the right to confiscate any items that it believes are being used irresponsibly.

ROLE OF OUR TECHNICAL STAFF

With the explosion in technology, the school recognises that blocking and barring sites is no longer adequate. Cobham Hall needs to teach all of its students to understand why they need to behave responsibly if they are to protect themselves. This aspect is the responsibility of the school's Safeguarding Lead and pastoral staff. The school's technical staff have a key role in maintaining a safe technical infrastructure at the school and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the school's hardware system, its data and for training the School's teaching and administrative staff in the use of ICT. They monitor the use of the internet and emails and will report inappropriate usage to the pastoral staff.

Access levels are reviewed to reflect the curriculum requirements and age of students.

ROLE OF OUR DESIGNATED SAFEGUARDING LEAD

Cobham Hall recognises that internet safety is a child protection and general safeguarding issue.

Mrs Carney, our Designated Safeguarding Lead (DSL) and other senior pastoral staff and Computing teachers have been trained in the safety issues involved with the misuse of the internet and other mobile electronic devices. The DSL liaises with Kent Safeguarding Children Board (KSCB) and other agencies in promoting a culture of responsible use of technology that is consistent with the ethos of Cobham Hall. All of the staff with pastoral responsibilities have also received training in e-safety issues provided by the Child Exploitation and Online Protection Command (CEOP). All year groups in the school are educated about the risks and the reasons why they need to behave

responsibly online and they are clear about expectations of appropriate and acceptable behaviour online. It is the DSL's responsibility to handle allegations of misuse of the internet.

MISUSE: STATEMENT OF POLICY

Cobham Hall will not tolerate any illegal material and will always report illegal activity to the police and/or the KSCB. If the school discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from CEOP or relevant safeguarding agencies. The school will impose a range of sanctions on any student who misuses technology to bully, harass or abuse another student in line with our anti-bullying policy.

INVOLVEMENT WITH PARENTS AND GUARDIANS

Cobham Hall seeks to work closely with parents and guardians in promoting a culture of e-safety. The school will always contact parents if it has any concerns about students' behaviour in this area and likewise it hopes that parents will feel able to share any concerns with the school. The school recognises that not all parents and guardians may feel equipped to protect their daughter when they use electronic equipment at home. The school, therefore, has arranged information sessions for parents when an outside specialist advises about the potential hazards of this exploding technology and the practical steps that parents can take to minimise the potential dangers to their daughters without curbing their natural enthusiasm and curiosity. Links to relevant information and guides are included on the school's website.

SAFE USE OF THE INTERNET AND ELECTRONIC DEVICES

E-safety is a whole school responsibility and at Cobham Hall the staff and students have adopted the following charter for the safe use of the internet inside the school:

Cyberbullying

- Cyberbullying is a particularly pernicious 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 school's anti-bullying policy describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying.
- Proper supervision of students plays an important part in creating a safe ICT environment at school but everyone needs to learn how to stay safe outside the school.
- Bullying and harassment in any form should always be reported to a member of staff. It is never the victim's fault, and she should not be afraid to come forward.

Treating Other Users with Respect

- The school expects students to treat staff and each other online with the same standards of consideration and good manners as they would in the course of face-to-face contact. Good behaviour is expected online as well as offline. They should always follow the 'IT Acceptable User Agreement' (see Appendix 1).
- The school expects a degree of formality in communications between staff and students and would not normally expect them to communicate with each other by text or mobile phones. The school's policy on educational visits explains the circumstances when communication by mobile phone may be appropriate. In such circumstances, school mobile phones are issued to staff. Parents will be made aware if other forms of internet based communications are to be used.
- Everyone has a right to feel secure and to be treated with respect, particularly the vulnerable. Harassment and bullying will not be tolerated. The school's anti-bullying policy is available on the school website. The school is strongly committed to promoting equal opportunities for all, regardless of race, gender, gender orientation or physical disability.
- All students are encouraged to look after each other and to report any concerns about the misuse of technology or worrying issue to a member of the pastoral staff.
- The use of cameras on mobile phones is not allowed in washing and changing areas.

Filtering

Internet access on the school's network is via a filtering system which permits blocking strategies that prevent access to a list of unsuitable sites. Maintenance of the blocking list by the school's IT Support department is a major task as new sites appear every day. A walled-garden or "allow-list" restricts access to a list of approved sites. Such lists inevitably limit students' access to a narrow range of information. Filtering examines web page content or e-mail for unsuitable words, this list is maintained externally and violations are reported to the Network Manager. Filtering of outgoing information such as web searches is also required. Rating systems give each web page a rating for sexual, profane, violent or other unacceptable content. Web browsers are set to reject these pages. The school uses Lightspeed Relay as a web filter. However, if staff or students discover unsuitable sites, the URL must be reported to the Network Manager. The school will continue to use appropriate filtering software on its network but has the ability to unblock specific sites for school use. Any breaches are reported immediately to the DSL.

Information Systems Security

Users must take responsibility for their network use. All users have unique network passwords known only to them which must be changed regularly. In addition, the school's management system (SIMS) has levels of access and passwords for individual users and all accounts information is on a separate, unconnected, system.

The security of the school information systems will be reviewed regularly. The school uses a combination of Trend Cloud App security and Microsoft Exchange Online Protection to automatically check uploaded and downloaded files originating from Office 365 and other cloud based solutions, this is automatically updated daily. Portable media is automatically checked for viruses on plug-in. Unapproved system utilities and executable files are not allowed in students' work areas or attached to e-mails. Files held on the school's network are checked daily. The school will continue to use appropriate anti-virus software.

E-mail

Spam, phishing and virus attachment can make e-mail dangerous. The school uses Trend Anti-Virus Solution to protect the network from cyberattack, viruses and Malware. Outgoing e-mails via the network are checked for viruses. Automatic daily updates are in place. Students must immediately tell a teacher if they receive offensive e-mail on the school system. Students are advised not to reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission. Access in school to external personal e-mail accounts may be blocked if they are found to be misused. Detailed guidelines for staff are published in the School Handbook; Section 6.6 – Use of telephone, email systems and internet.

Social Networking and Personal Publishing

Parents and teachers need to be aware that the Internet has emerging online spaces and social networks which allow individuals to publish unmediated content. Students are encouraged to think about the ease of uploading personal information and the impossibility of removing an inappropriate photo or address once published. Examples include: blogs, wikis, forums, live streaming, bulletin boards, multi-player online gaming, chat rooms, instant messenger and many others.

- The school will filter access to social networking sites for all years and block access to sites until students are old enough to be members of that site. Currently, the recommendation is 13 for most sites, however, WhatsApp is 16.
- Students are advised never to give out personal details of any kind which may identify them and/or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and e-mail addresses, full names of friends, specific interests etc.
- Students will be advised to be careful about placing personal photos on any social network space. Advice will be given regarding background detail in a photograph which could identify the student or her location, e.g. house number, street name or school.

- Students will be advised on security and encouraged to set passwords, deny access to unknown individuals and instructed how to block unwanted communications.
- Students will be encouraged to invite known friends only and deny access to others.
- Students will be advised not to publish specific and detailed private thoughts. The school is aware that bullying can take place through social networking especially when a space has been setup without a password and others are invited to see the bully's comments (see also Anti-Bullying Policy).

Staff should not add current students to their social networking sites other than systems set up by the school for teaching and learning that should have built in user authentication and archiving. Neither should staff accept invitations to join a current student's social networking site. Students who make such invitations should be warned by pastoral staff about the inappropriateness of their actions.

Staff should also be cautious of adding recent former students to their social networking sites as they may provide an indirect link to current students.

Staff should also be cautious of adding current parents to their social networking sites as they may provide an indirect link to current students.

Detailed guidelines for staff are published in the School Handbook; Section 6.6 Social Media policy.

Promoting Safe Use of Technology

Students of all ages are encouraged to make use of the excellent online resources that are available from sites such as:

- UK Council for Child Internet Safety (http://www.education.gov.uk/ukccis)
- Childnet (www.childnet.com)
- Cyberbullying (https://cyberbullying.org)
- Bullying UK (www.bullying.co.uk)
- Child Exploitation and Online Protection (www.ceop.police.uk)

They prepare their own models of good practice which form the subject of presentations during assemblies and discussion in the meetings of the school council. They cover the different hazards on the internet, such as grooming, stalking, abuse, bullying, harassment, identity theft and online reputation. Guidance covers topics such as saving oneself from future embarrassment explaining that any blog or photograph posted onto the internet is there permanently. Anything that has been deleted may be cached in a search engine, company server or internet archive and cause embarrassment years later.

Safe Use of Personal Electronic Equipment

- The school's guidance is that students and staff should always think carefully before they post any information online. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.
- The school offers guidance on the safe use of social networking sites and cyberbullying in Wellbeing lessons which covers blocking and removing contacts from 'friend lists'.
- The school's Wellbeing lessons include guidance on how students can identify the signs of a cyber-stalker and what they should do if they are worried about being harassed or stalked online.
- The school offers guidance on keeping names, addresses, passwords, mobile phone numbers and other personal details safe. Privacy is essential in the e-world.
- The school gives guidance on how to keep safe at home by not opening unknown attachments and reporting any illegal content.
- Similarly the school covers how a mobile phone filter can be activated and how to block nuisance callers.
- The school appreciates that free video calls can provide boarders with an invaluable means of maintaining contact with their families and friends. The school advises on the responsible use of such apps.

Considerate Use of Electronic Equipment

- Mobile phones, tablets and other personal electronic devices should be switched off and stored securely during the school day, unless being used at the direction of a teacher in a lesson. They may be used during lunch-times in designated areas and in boarding houses after school.
- Staff may confiscate personal equipment that is being used inappropriately during the school day.
- Sanctions may be imposed on students who use their electronic equipment without consideration for others.
- There is now an increasing body of evidence that using light emitting devices immediately before bedtime affects sleep patterns[1]:
    - Years 7 to 10 boarders hand in all electronic equipment at bedtime.
    - Wi-Fi access to the internet is timed to shut down at 22:00 for Years 7 to 10, 22:30 for Year 11 and midnight for Years 12 and 13.

Emerging Technologies

Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, wide Internet access and multimedia. A risk assessment needs to be undertaken on each new technology and effective practice in classroom use developed. The safety and effectiveness of wider virtual communities depends on users being trusted and identifiable. This may not be easy, as authentication beyond the school may be difficult as demonstrated by social networking sites such as Facebook. Such technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. The school cannot accept liability for the material accessed, or any consequences resulting from Internet use.

Related Policies and Documents

- Policy Statement on Anti-bullying
- Policy Statement on Taking, Storing and Using Images of Children
- Policy Statement on Behaviour and Discipline
- Policy Statement on Safeguarding
- Policy Statement on Data Protection
- Policy Statement on Internet Misuse involving Outside Lets
- Policy Statement on Social Media
- Policy Statement on Electronic Devices
- Wellbeing Scheme of Work
- Staff Handbook

[1] *www.pnas.org/content/early/2014/12/18/1418490112. Accessed 19/01/2015. Evening use of light-emitting eReaders negatively affects sleep, circadian timing, and next-morning alertness.]*

APPENDIX 1 **IT ACCEPTABLE USER AGREEMENT** **SEPTEMBER 2021**

1) I will work in a quiet and responsible manner on all computers and will not disturb other students. I will not leave books or rubbish around the computer rooms and will treat all equipment and facilities with respect. I will not eat or drink near a computer. Any damage should be reported.

2) I will not divulge any usernames or passwords to anyone, including my photocopier PIN and WiFi key. I will also not log on to any system using other users log on details. I understand that by doing so may be a criminal offence under the Computer Misuse Act 1990.

3) I will not open e-mail messages or attachments from people I do not know as I could accidently:
   a) Introduce a virus to the system
   b) See inappropriate material
   c) Be traced and tracked by someone I don't know

4) I am aware that use of any ICT system during school time is for educational purposes only. I will abide by all School policies relating to the use of electronic devices.

5) I will use all forms of technology responsibly and sensibly including, but not exclusive to, all forms of Social Media, Communication systems, mobile devices and Apps.

6) I will not use any forms of equipment for any of the following:
   a) Bullying
   b) Causing offence, upset or embarrassment to other people, both inside and outside Cobham Hall. This includes fellow students and teachers.
   c) I will not post pictures or videos of people without their permission.
   d) I will not make contact with people that I do not know.
   e) I will not share or enable others to access my personal Wi-Fi via a Hot Spot.

   I understand that if I breach points a, b or c I may be committing a criminal offence under the Defamation Act 1996 and/or the Communications Act 2003.

7) I will alert a member of staff if:
   a) Someone contacts me who I do not know.
   b) I am being bullied.
   c) I see inappropriate pictures or messages.

8) I will not download or stream any copyrighted material from the internet without permission whilst at school as I could be committing a criminal offence under the Copyright and Patents Act of 1988. I will not use material from the internet in my schoolwork without first making sure I am allowed to do so. I will ask a teacher if I am unsure.

9) I will not download or upload any material that could be considered illegal or offensive. If I come across anything that may be offensive or illegal, I am to notify a teacher immediately.

10) I am aware that all internet activity is logged by the school and authorised staff may monitor any usage to the extent permitted by law.

11) I will not attempt to bypass the school's internet filtering or security systems.

12) I will make sure that all ICT communications are responsible, sensible and fitting to the school ethos.

Name of Student: ..... Signature: .....

Updated : September 2021
Approved by Governors :
Review Date : September 2022