STUDENT E-SAFETY (or COMPUTER AND NETWORK ACCESS) POLICY

OUR POLICY

Concord College aims to provide a first class education for its students, but also recognises that the majority of its students need to have time and access to facilities for recreation and relaxation. While the College recognises that some students enjoy playing computer games in their spare time, the academic life and work of the College must remain at all times the number one priority in terms of the work of the IT department and the College's computer network.

Another extremely important function of the College network is to enable boarding students to maintain contact with family and friends. On the other hand, students need to have adequate and quality sleep in order to be able to learn effectively and thus they should not be skyping or social networking late into the night. It is for this reason that wi-fi access in boarding houses via the College network is suspended between midnight and 6am each day.

ICT IN THE CURRICULUM

Technology has transformed the entire process of teaching and learning at Concord College. It is a crucial component of every academic subject and is also taught as a subject in its own right. The College's classrooms are equipped with electronic whiteboards, projectors and computers. Concord College has dedicated mobile fleets of Microsoft Surface Pros as well as other computers located in boarding houses and common rooms. In addition, there are additional computers located in the library for private study. All of the College's buildings, including each student bedroom in its boarding houses, are wi-fi enabled to allow access to the Internet.

All of Concord College's pupils 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 websites that appear to be serious, impartial, historical sites, actually masquerade as sources of racist, homophobic, jihadist or other propaganda. Some free, online encyclopaedias do not evaluate or screen the material posted on them.

THE ROLE OF TECHNOLOGY IN OUR PUPILS' LIVES

Technology plays an enormously important part in the lives of all young people. Sophisticated games consoles, together with bluetooth-enabled mobile phones provide unlimited access to the internet, to SMS messages, to blogging (web logging), to social media websites (like X – formally Twitter), to Skype (video calls, via web cameras built into computers, phones and games consoles), to wikis (collaborative web pages), chat rooms and other social networking sites (such as Bebo, Facebook and TikTok), and video sharing sites (such as YouTube).

This communications revolution gives young people unrivalled opportunities. It also brings risks. It is an important part of the College's role to teach pupils 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.

ROLE OF OUR ICT DEPARTMENT

With the rapid and continued rate of development in technology, the College recognises that blocking and barring sites is no longer adequate on its own although filters are in place on the College network. Concord College needs to teach all of its pupils to understand why they need to behave responsibly if they are to protect themselves. This responsibility is met through the College's PSHE programme and is also a role for the Vice-Principal (Pastoral) & Designated Safeguarding Lead. The College's technical staff have a key role in maintaining a safe technical infrastructure at the College and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of the College's hardware system, its data and for training the College'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 Vice-Principal (Pastoral) & other Pastoral Team Managers.

ROLE OF OUR DESIGNATED SAFEGUARDING LEAD (or DSL)

Concord College recognises that internet safety is a child protection and general safeguarding issue.

The Vice-Principal (Pastoral) & Designated Safeguarding Lead at Concord College holds responsibility for safety issues involved with the misuse of the Internet and other mobile electronic devices. He liaises closely with the Local Safeguarding Children Board (LSCB) and other agencies (such as CEOP) in promoting a culture of responsible use of technology that is consistent with the ethos of Concord College. Teaching and pastoral staff have received NOS (National Online Safety) training and guidance in e-safety issues – including the dangers of cyberbullying. The College's PSHE programme will ensure that all year groups in the College are educated in the risks and the reasons why they need to behave responsibly online. It is the Vice-Principal (Pastoral) & Designated Safeguarding Lead's responsibility to handle allegations of misuse of the internet.

MISUSE: STATEMENT OF POLICY

Concord College will not tolerate any illegal material and will always report illegal activity to the police and/or the LSCB. If the College discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from the Child Exploitation and Online Protection Unit (CEOP). The College will impose a range of sanctions on any pupil who misuses technology to bully, harass or abuse another pupil in line with our anti-bullying policy. See below for an extract from Staff handbook doc. 4.2.a "Sanctions – A General Guide & Tariff".

19	**COMPUTER USAGE OFFENCES**
	• Minor breaches (e.g. sending spam emails, obtaining the password to the staff wifi and using it, bypassing College security mechanisms – including the use of VPNs. Inoffensive, but annoying breaches.) **First offence** - Double / triple detention. Verbal warning. **Second offence** - 2x Saturday afternoon triple detention. Letter to parents. Formal warning. Confiscation of devices for 7 days

	Third offence - Internal suspension of 1 or 2 days. Letter to parent & final warning. Confiscation of devices for 14 days. • Serious breaches (e.g. sending offensive/ abusive e-mails, hacking, cyberbullying, illegal activities, posting on the internet anything which brings the good name of the College into disrepute) **First offence** - Internal suspension of 1 or 2 days. Letter to parent & formal warning about further offences bringing the student's future at the College into doubt. However, in the case of a very serious breach of College discipline (e.g. cyberbullying of another student), a serious punishment - such as being expelled or being required to leave – could be applied even for a first offence. **Second offence** - A final warning to both the student as well as a letter to parents combined with a 14 day suspension will usually be given, but the seriousness of the offence might result in the student being expelled or being required to leave. **Third offence** - The student will be required to leave the College. (Expulsion might be applied if the gravity of the offence is deemed to warrant it.)

INVOLVEMENT WITH PARENTS AND GUARDIANS

Concord College seeks to work closely with parents and guardians in promoting a culture of e-safety. The College 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 College.

CHARTER FOR THE SAFE USE OF THE INTERNET AND ELECTRONIC DEVICES AT CONCORD COLLEGE

"Children and young people need to be empowered to keep themselves safe - this isn't just about a top-down approach. Children will be children - pushing boundaries and taking risks. At a public swimming pool we have gates, put up signs, have lifeguards and shallow ends; but we also teach children how to swim."

Dr Tanya Byron "Safer Children in a digital world: the report of the Byron Review".

E-safety is a whole College responsibility and at Concord College the staff and pupils have adopted the following charter for the safe use of the internet inside the College:

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 College's anti-bullying policy describes the preventative measures and the procedures that will be followed when the College discovers cases of bullying.
- Proper supervision of pupils plays an important part in creating a safe ICT environment at College but everyone needs to learn how to stay safe outside the College.
- Concord College values all of its pupils equally. It is part of the College'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 College expects pupils 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.

- The College 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 use College, as opposed to personal, mobiles and pupils' mobile numbers are deleted at the end of the visit.

- 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 College's Anti-Bullying Policy. The College 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 to report any concerns about the misuse of technology or worrying issue to a member of staff.

- The use of cameras on mobile phones is not allowed in washing and changing areas. Careful thought needs to be given before using them in the bedrooms of boarding houses.

Not Bringing the College into Disrepute

- Students must not use the logo, other branding, or name of "Concord College" on social media or websites without specific permission having first been obtained from the Principal or his deputy. Students must not bring the good name of the College into disrepute by their actions, online messages, or posts.

Build a positive online reputation

- Students should consider the long-term impact of what they post online. Future employers and universities are likely to conduct online searches of prospective employees/ students. Students should be positive and build their "brand". Remember that if you post something linked to your name, your reputation could be damaged or enhanced accordingly.

- Students should also check their privacy settings on social media.

Keeping the College Network Safe

- The College adheres to best practice regarding e-teaching and the internet.

- Certain sites are blocked by the College's filtering system and the College's IT department monitors pupils' use of the network.

- The ICT department monitors email traffic and blocks SPAM and certain attachments.

- The College issues all pupils with their own personal College email address. Access is via personal LOGIN, which is password protected. The College gives guidance on the reasons for always logging off and for keeping all passwords securely. Student usernames and passwords must **not** be shared by students with anyone else (including their parents) unless required to do so by Concord staff. Sharing access is a breach of College rules and is likely to result in disciplinary action.

- Access to some sites is not allowed on the College's network.

- The College has class leading anti-virus and monitored threat response protection on its network which is operated by the ICT department in conjunction with a highly respected third party security vendor.

- Any member of staff or pupil who wishes to connect a removable device to the College's network is asked to arrange in advance with the ICT department to check it for viruses and to ensure compliance with the College's data encryption policy.

Promoting Safe Use of Technology

Pupils 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 International (www.childnet-int.org)
- Cyber Mentors (www.cybermentors.org.uk)
- Cyberbullying (www.cyberbullying.org)
- E-Victims (www.e-victims.org)
- Bullying UK (www.bullying.co.uk)

PSHE lessons and assemblies cover the different hazards on the Internet, such as grooming, stalking, abuse, bullying, harassment and identity theft. 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 College's guidance is that pupils 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. Posts could also impact on the reputation of individuals and the wider College community. Students should not bring the good name of the College into disrepute since they will be in breach of our rules and face sanctions.
- The College offers guidance on the safe use of social networking sites and cyberbullying in PSHE lessons which covers blocking and removing contacts from 'friend lists'.
- The College's PSHE lessons 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 College offers guidance on keeping names, addresses, passwords, mobile phone numbers and other personal details safe. Privacy is essential in the e-world.
- The College gives guidance on how to keep safe at home by encrypting the home wireless network, not opening unknown attachments and reporting any illegal content.
- The College advises on the responsible use of Skype. However, it appreciates that free video calls can provide boarders, particularly overseas boarders, with an invaluable means of maintaining contact with their families and friends.
- The College recognises the increasing use of video chat and live streaming for academic purposes – such as remote learning, online Tutoring & interviews. However, there are safeguarding risks involved.

  All Concord College students must:

  i. inform parents and College staff (- usually their personal tutor) in advance of such sessions taking place;

ii. record, where possible, such sessions in case there are problems and footage can then be reviewed as needed (- the permission of the other party should always be gained before any such recording takes place);

iii. be prepared to end online sessions if they become concerned about inappropriate behaviour & then to report this to College staff;

iv. note that all e-mails, chat messages or video-bases lessons conducted via Teams involved in remote learning (or other communications) with Concord staff are recorded and will be reviewed in the event of any concerns being raised;

v. dress appropriately as they would for the academic day and be seated at their desk and ready to learn via video link (& not be in their pyjamas or in bed).

Important note: With the exception of College sanctioned remote learning sessions, Lower School Students must also conduct sessions in public areas of the College where staff supervision is available (e.g. Lower School boarding residence common rooms, the careers room in the library).

Considerate Use of Electronic Equipment

- Mobile phones, smart phones, ipods and other personal electronic devices should be switched off and stored securely during the academic day. They may be used during break times. However, mobiles should be switched off or switched to silent mode during assemblies, registration times, lessons etc.

- Staff may confiscate personal equipment that is being used inappropriately during the College day for periods of up to 14 days. (Please see the separate Policy & Procedure on Confiscation for more details.) In the event that a password protected electronic device is confiscated, & the confiscation is due to suspicions of usage which is in breach of the "Student Computer & Network Access Policy", students must be willing to share passwords in order 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 use their electronic equipment without consideration for others.

Concord College expects all pupils to adhere to this charter for the safe use of the Internet. Use of the College network by students is dependent upon their compliance with this policy on acceptable use. All students are asked to sign up to this policy annually on SharePointand a copy is made available to parents via the College's website, and the College may impose sanctions for the misuse, or attempted misuse of the internet, mobile phones and other electronic devices.

Computer Gaming at Concord College

Although some computer gaming can be argued to bring some educational and social benefits to students, it must also be recognised that computer gaming can be a distraction from other more important tasks and can have a negative impact on students' academic progress. In line with the College's stated aims, students are encouraged to learn self-discipline and self-regulate the amount of time they devote to pursuits such as gaming, social networking and so on.

The College recognises its duty of care to both its students and their parents. College staff act in loco parentis for students who might need restrictions imposed on them if they spend an unhealthy amount of time on any activity which means they are not getting enough sleep or which leads to a negative impact on their personal or academic development.

During the academic working day, students should not use the College network for computer gaming or to download anything which might take up bandwidth needed for the smooth and fast operation of the system so that the College's academic objectives can be achieved. Computer gaming should be limited to students' free time (i.e. after lessons, after prep sessions, at weekends). It is the recommendation of the College that students should spend very little time gaming during the working week.

Procedures:

As stated above, it is hoped that students will act responsibly at all times, but the College recognises the need to have measures in place to prevent students suffering from the addictive nature of computer gaming and consequent under-achievement and/or health problems. Staff and students at the College should be aware of the following:

1) Confiscate students' laptops, tablets, smartphones or other mobile devices where there is concern that they are not making best use of their free time. Such confiscations will usually last for 14 days in the first instance and parents will normally be informed of the reasons for such confiscations. (Please see the separate Policy & Procedure on Confiscation for more details.)

2) Students gaming during the academic day will be subject to disciplinary measures – such as a detention.

3) Students must recognise that the primary function of the College network is to enable the College to achieve its academic aims. Students must not, therefore, take up Internet bandwidth during the academic day with non-academic activities (e.g. by downloading games or streaming films). Disciplinary action will be taken and students could have their access to the College's computer network suspended for a period of time, or even removed completely. Their student accounts could be disabled.

4) Boarding students must not play computer games after room checks in boarding houses. Indeed, House Parents & Night Security Personnel/ Night Pastoral Staff are to be vigilant for students whose use of modern technologies might lead to disrupted, or insufficient sleep, due to over-stimulation in the 40-60 minute period before going to bed.

5) The College has the right to monitor students' activities over its computer network and to intervene when staff believe that student activities are having a negative impact on the operation of the network, or when students are not acting in accordance with this policy.

6) Computer games will not be installed/ will be removed from the College network if there are any concerns about their suitability or safety for students. In making such decisions, the College will always err on the side of caution in seeking to protect its students from the potential dangers posed by the internet (e.g. abusive exchanges between player online, trolling, grooming by paedophiles). Such decisions will be taken by ICT staff in consultation with the Children's Safeguards Manager and/ or other members of the Senior Management Team.

Data Protection, Privacy & Monitoring

The College has appointed the Assistant Bursar (Finance & Operations) as the Data Protection Officer, who can be contacted if you have any concerns with data protection at dataprotectionofficer@concordcollege.org.uk or by telephone: (01694) 731836. New data protection legislation provides further rights for data subjects (students); the legislation has been modified in some areas and has been a completely new addition in other areas. For more information, please visit the College website which contains the College's Privacy Policy. In addition, a student

version of our Data Protection Policy is saved as document 11 in the Student Handbook on the O drive.

The College monitors the usage of its network to ensure compliance with legislation in force from time to time, examples comprise:

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

STUDENTS SHOULD TAKE NOTE OF THE FOLLOWING RULES & INFORMATION RELATING TO USE OF THE COLLEGE'S COMPUTER NETWORK:

1. The networks shall not be used for transmission or receipt of information that promotes:
   - Discrimination on the basis of race, creed, colour, gender, religion, disability or sexual orientation
   - Sexual harassment
   - Copyright infringement (including illegal music or video downloads)
   - Cyberbullying
   - Trolling (i.e. annoying behaviours - such as sending spam e-mails)
   - Personal business interests

   OR
   - Any unlawful activity (e.g. grooming)

2. The Concord College ICT Network shall not be used to send or receive anything where the content and/or meaning of the material are likely to be deemed obscene, abusive or highly offensive to recipient(s). This rule prohibits students from sending "spoof" e-mails to recipients.

3. Users of the Concord College ICT Network Services shall respect the rights and property of all others and shall not attempt to improperly access, misappropriate or misuse the network accounts/information/files of other users. (Examples of misuse of the network include: students taking insufficient care to log off their accounts when working on computers in public areas of the College; using other students' accounts to send "spoof" e-mails.)

4. Users of Concord College Network Services will act responsibly at all times. Examples of irresponsible use include, but are not limited to:

   - Installing or attempting to install unlicensed or untested software or hardware.

   - Tampering with and damaging hardware. (For example, unplugging cables from desktop computers in public areas of the College – such as the library, student common rooms and classrooms.)

   - Using on-line Chat facilities (Chatlines).

   - Playing games or shopping online is forbidden on desktops located within academic areas of the College – including the library.

   - Attempting to bypass the protective College's filtering or anti-virus software. (For example, using proxy servers, or VPNs, to gain unfiltered access to the Internet is not allowed.)

   - Accessing pornographic or inappropriate materials.

- Students should exercise particular care when posting comments and photographs on social media sites (e.g. Facebook). The College expects pupils 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. Students should make sure that nothing posted can be construed as cyberbullying.

- Accessing online dating sites. Dating sites are blocked over the College network. There are very real risks in meeting individuals first met online in the real world.

5. The Network shall not be used for commercial purposes. Advertising of unauthorised commercial offerings is forbidden.

6. Any individual who abuses, or who gains unauthorised access to, the College's computer resources will be subject to disciplinary action. It might also be that in cases of serious breaches of this policy that appropriate authorities (i.e. the Police) will be involved.

7. Misuse of the Concord College ICT Network can have a negative impact upon individuals, groups of students and staff and the reputation of the college. Concord College has an Internet and email filtering system which monitors all users' activity on the Network. We, therefore, maintain the right to monitor all internet usage and check upon the use and content of e-mails. The College reserves the right to conduct an audit at any time to ensure compliance with this policy.

Disclaimer

1. Concord College 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 Concord College or its staff.

2. Concord College is not responsible for the quality, accuracy or content of any materials that an individual user may make available within or outside the Concord College through the Network.

3. Concord College is not responsible for the provision of Internet services that are supplied by a third party. However Concord College will make every endeavour to ensure continuity of service.

4. Despite the College investing in considerable improvements to its internet service, wi-fi coverage and available bandwidth over the past few years, it cannot guarantee bandwidth to student users at any given time.

5. While being prepared to make reasonable adjustments where possible, the College does not guarantee that all devices (e.g. Windows 'phones & Kindles) will be fully compatible with its systems.

6. The College does not undertake to repair students' own computer equipment – such as personal laptops. It might be possible to assist students in getting their equipment repaired by third parties, but Concord does not offer any guarantee in terms of those services or repairs.

7. Given the College's rural location, students should note that both mobile signal coverage and strength of mobile signal are beyond our control. (At present, O2, EE and Orange provide the best service and signal strength.)