

## **STUDENT E-SAFETY POLICY**

### **Summer School**



Concord College aims to provide a first-class experience for its students, including having time and access to facilities for recreation and relaxation after lessons. The College recognises that some students enjoy playing computer games in their spare time, however staff will monitor computer usage to ensure that students have time away from screens. We know access to technology is vital to enable students to maintain contact with family and friends whilst they are away from home.

However, students need to have adequate and quality sleep to be able to learn effectively and thus they should not be making video calls, web searching or using social networks 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.

The College's classrooms are equipped with electronic whiteboards, projectors and a computer for teachers use. The College makes use of fold-away desk units which store computers neatly out of sight when they are not being used in the student social space, The West End. Concord College has 2 dedicated ICT classrooms as well as other computers located in some boarding residences and common rooms. All the College's buildings, including its boarding residences, have wi-fi enabling access to the internet.

It is important to teach students 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. Students will attend an orientation session covering online safety whilst at Summer School.

### **ROLE OF OUR IT DEPARTMENT**

With the explosion 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 students to understand why they need to behave responsibly if they are to protect themselves. This responsibility will be met via the orientation sessions and the Summer School's 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 Summer School Designated Safeguarding Lead.

Concord College recognises that internet safety is a child protection and general safeguarding issue and the Summer School Designated Safeguarding Lead at Concord College holds responsibility for safety issues involved with the misuse of the internet and other mobile electronic devices. Summer School teachers and the Safeguarding Team have received National Online Safety training and guidance in e-safety issues as part of their induction training.

## **MISUSE: STATEMENT OF POLICY**

Concord College will not tolerate any illegal material and will always report illegal activity to the

Page 1 of 7

Rev Jun 21

police. If the College discovers that a student is at risk because 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 student who misuses technology to bully, harass or abuse another student in line with the Summer School's *Abusive Behaviour & Anti-Bullying Policy*.

## **INVOLVEMENT WITH PARENTS AND GUARDIANS**

The College 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 College.

Page 2 of 7

Rev Jun 21

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

### **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 *Abusive Behaviour & Anti-Bullying Policy* describes the preventative measures and the procedures that will be followed when the College discovers cases of bullying.
- Proper supervision of students 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 its students 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 students 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 College 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. On educational visits, when communication by mobile phone may be appropriate, staff use College, as opposed to personal, mobiles and students' 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 Summer Schools *Abusive Behaviour & Anti-Bullying Policy*. The College 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 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 residences.

### **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 Course Director or Assistant Course Director. 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.

Page 3 of 7

Rev Jun 21

### **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 students' use of the network.
- The IT department monitors email traffic and blocks SPAM and certain attachments.
- The College issues all students 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.
- Access to some sites is not allowed on the College's network.
- The College has strong anti-virus protection on its network which is operated by the IT department.
- Any member of staff or student who wishes to connect a removable device to the College's network is asked to arrange in advance with the IT department to check it for viruses and to ensure compliance with the College's data encryption policy.

### **Safe Use of Personal Electronic Equipment**

- The College'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.

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 orientation lessons which covers blocking and removing contacts from 'friend lists'.
- The College's orientation 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 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 advises on the responsible use of Skype. However, it appreciates that free video calls can provide students with an invaluable means of maintaining contact with their families and friends.

### **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 lessons and activities etc.
- Staff may confiscate personal equipment that is being used inappropriately during the College day until the end of the lesson or the end of the day. In the event that a password protected electronic device is confiscated, and the confiscation is due to suspicions of usage which is in breach of the *Student E-Safety 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 students who use their electronic equipment without consideration for others.

Concord College expects all students 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.

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](mailto: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 Summer School [website](#) which contains the College's Privacy Policy.

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

Page 5 of 7

Rev Jun 21

## **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 based on 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
  - 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 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.
  - 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 students to treat staff and each other online with the same standards of consideration and good manners as they would during face-to-face contact. Students should make sure that nothing posted can be construed as cyberbullying.
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.

Rev Jun 21

## 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.)

Adapted from Concord College Main Term Policy Section 9

<b>Document Owner</b>	Summer School
<b>Reviewed in</b>	June 2025 SB
<b>Approved by/date</b>	KQ/03/08/2021
<b>Next review</b>	June 2026



<b>Publication</b>	Portal & Website
--------------------	---------------------