COLLINGHAM
KENSINGTON

# E-SAFETY POLICY AND PROCEDURES
## including the Acceptable Use of ICT and Cyber Bullying

**Introduction**
The primary purpose of this policy is to safeguard students and staff at Collingham College. It details the actions and behaviour required from students and members of staff in order to maintain an e-safe environment. Key messages to keep children and young people safe are to be promoted and should be applied to both online and offline behaviours.

Our e-Safety Policy has been written based on government guidance. Our nominated e-Safety Officer is Sally Powell. This role overlaps with that of the Designated Safeguarding Officer role. It is not a technical role. The primary purpose of this policy is to safeguard students and staff at our college. It details the actions and behaviour required from students and members of staff in order to maintain as safe an environment as possible.

The breadth of issues classified within online safety is considerable and ever evolving, but the college's approach recognizes four main areas of risk:

- content: being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- contact: being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- conduct: online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g. consensual and nonconsensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and
- commerce: - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel students or staff are at risk, the Principal will report it to the Anti-Phishing Working Group (https://apwg.org/).

Collingham College provides an environment in which children, parents and staff are safe from images being recorded and inappropriately used. The word 'camera' in this document refers to any device that may be used to take and store a digital image e.g. mobile phone, tablet, laptop etc.

All staff, across the college community, contribute to the E-Safety Policy and the responsibilities are shared. Any technology used in college (regardless of ownership) shall be governed by this policy. This policy should also be read in conjunction with the Anti-Bullying Policy. Networked computer resources and internet access are widely available at the college. All those who wish to use the system must comply with this policy. In accordance with legislative requirements, we have a whole college approach to e-safety.

**For Students:**
Students at Collingham College will be given supervised access to our computing facilities and will be provided with access to filtered internet and other services operating at the college. The promotion of online safety within ICT activities is to be considered essential for meeting the learning and development needs of children and young people. Key messages to keep children and young people safe are to be promoted and should be applied to both online and offline behaviours.

**Health and Safety Policy**
The safe use of ICT is included within the Health and Safety Policy, and should also include guidelines for the use of display screen equipment.

**Why is Internet use important?**
All children deserve the opportunity to achieve their full potential; in our modern society this should incorporate the use of "Appropriate and Safe" ICT facilities including online resources and services. In order for the college to maintain such an environment for learners (children and adults) everybody must be aware of the need to ensure on-line protection (E-Safety) and subsequently understand the principles of this policy and the expectations of college practice as documented below.

Having internet access enables students to explore thousands of global libraries, databases and bulletin boards. Collingham monitors the use of its computers and automatically blocks some sites. However, parents need to be aware that despite the college's best endeavours, some students may find ways to access material that is inaccurate, defamatory, illegal or potentially offensive to some people.

However, at Collingham College we believe that the benefits to students having access to the internet in the form of information, resources and opportunities for collaboration exceed any disadvantages. Although, as with any other area, parents and guardians of minors along with the college share the responsibility for setting and conveying the standards that students should follow when accessing and using these media information sources at college and/or at home. During college time, teachers will guide students towards appropriate material on the internet. Outside college, families bear the same responsibility for guidance as they exercise with other information sources such as television, telephones, films and radio etc.

**Access to Computers:**
- Access to the college network is available from any network station during the normal college day.
- Access to the college network will be provided for students to carry out recognised college work, but only on the understanding that they agree to follow our guidelines. These guidelines apply both to students and staff.
- Intentional damage caused to a computer, computer systems or networks including unauthorised damage or interference with any files is not permitted and may be considered a criminal offence under the Computer Misuse Act 1990.
- The unauthorised access or use of personal information, contrary to the provisions of the Data Protection Act is not permitted.
- College ICT systems security will be reviewed regularly.
- Virus protection will be updated regularly.
  If a 'virus alert' occurs when transferring work from one mode to another the IT technician should be informed immediately. All external hardware e.g. Memory sticks must be vetted by submitting them to an anti-virus check.
- Security strategies will be discussed at staff meetings.

**Protecting Personal Data:**
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

**E-mail /Teams Usage:**
- Staff at Collingham College are provided with a college email address which they should use in any correspondence with students or parents.
- Staff should exercise extreme caution when referring to students' confidential details by e-mail and avoid making such references whenever possible. In situations when it is necessary, the e-mail should be marked CONFIDENTIAL and initials should be used rather than full names.
- Staff must not reply if they receive an offensive e-mail and must immediately inform a member of SLT.
- Students must immediately tell their Personal Tutor if they receive an offensive e-mail or other electronic message.
- Staff must copy in the Personal Tutor and/or the Principal into any e-mail correspondence with students or parents.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The forwarding of chain letters or the sending of group emails within the college and without permission is not permitted.

- Staff may message students using Teams but they may not call (video/call) them outside of their lesson time without previously notifying the Personal Tutor or member of the SLT of the date/time and reason for doing so. Teams should only be used with regard to the college's Online Teaching and Learning Policy.

**Mobile Phones**
- At no time should staff use their personal phones to telephone students or store students' numbers.
- Staff supervising college outings will be provided with a Collingham phone and only the number of this phone should be given to students on the trip.

**Published content and the college website:**
- Staff or student personal contact information will not be published on the college website. The only contact details given on our website will be the college address and telephone number.
- We may use photographs of children in newsletters and in the college prospectus.
- Photographs will be checked to ensure that they are suitable.
- Photographs and videos may only be uploaded to the college website with the Principal's approval.
- Photographs are used in and around the college for many purposes, records of practical work (e.g. art or technology projects) and records of important college events.

When students join Collingham College, as part of our registration process, we ask parents to give consent for photographs and videos to be taken for college marketing purposes. If consent is withheld, such photographs/videos are not published of the individual child concerned. Full information about the use and processing of personal data along with relevant contacts can be found in our Privacy Policy.

**Social networking:**
- The college will not allow access to social networking sites such as Facebook, Instagram or Twitter for students or staff.
- Students will be advised never to give out their personal details of any kind which may identify them, their friends or their location.
- Staff should never contact students via social networking nor respond to student requests to 'friend' or follow them.

**Peer on Peer Abuse:**
Sexting, the sharing of nudes or semi-nude images/videos, is a child protection issue. Even if explicit material is sent or elicited without malicious intent the consequences are serious and put those involved at risk of serious harm. Having or sending explicit material on digital devices is also a criminal offence for those under 18. Pupils are taught about sexting as part of their internet safety education. The colleges takes incidences of sexting extremely seriously, and deals with them in accordance with child protection procedures, including reporting to the police.

**Assessing Risks:**
- We will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the college network. The college cannot accept liability for any material accessed, or any consequences of internet access.
- Mobile phones with internet access (smartphones) are not governed by the college's infrastructure and bypass any and all security and filtering measures that are or could be deployed.
- We will audit ICT use to establish if the e-Safety policy is sufficiently robust and that the implementation of the e-safety policy is appropriate and effective.
- Methods to identify, assess and minimise risks will be reviewed regularly.

**Reporting of issues and concerns**
Collingham College has clear reporting mechanisms in place and available for all users to report issues and concerns. For staff, any concerns regarding e-safety should be made to the Deputy Principal or Principal who will review the issue and take the appropriate action. For students, they should raise any concerns with their teacher or Personal Tutor who will then pass this on to the Deputy Principal.

**How will the policy be introduced to students?**

- Students will be informed that internet use will be monitored.
- A module on responsible internet use will be included in the PSHE programme covering both home and college use.
- Students will be informed that network, Microsoft Teams and internet use will be monitored and appropriately followed up.

**How will staff be consulted and made aware of this policy?**

- All new staff will be taken through the key parts of this policy as part of their induction.
- All staff will be provided with this policy and have its importance explained as part of the child protection training requirement.
- Staff will be informed that network and internet traffic can be monitored and traced to the individual user.
- Staff development in safe and responsible internet use and on the college Internet policy will be provided as required.
- Breaching this e-safety policy may result in disciplinary action being taken and access to ICT being restricted or removed.

**How will ICT system security be maintained?**

- The college ICT systems will be reviewed regularly with regard to security
- Security strategies will be discussed at staff meetings.
- Virus protection will be installed and updated regularly.
- Personal data sent over the internet will be encrypted or otherwise secured.
- Use of portable media such as floppy disks, memory sticks and CD-ROMs will be reviewed and its content can be searched by a member of staff.
- Files held on the college network will be regularly checked.
- All network system and administration passwords are to be recorded by the Deputy Principal and kept in a secure place.
- Staff will ensure that student data is held only on cloud based secure systems, such as Microsoft Teams, Outlook, CPOMS and Celcat.
- The college will ensure that access to all its ICT systems will be denied to staff at the end of their employment with the college.

**How will complaints regarding Internet use be handled?**

- The Deputy Principal is responsible for handling incidents.
- Complaints of internet misuse will be dealt with by the Principal.
- Any complaint about staff misuse must be referred to the Principal.
- Complaints of a child protection nature must be dealt with in accordance with our child protection procedures.
- Students and parents will be informed of the complaint procedure.
- As with drug issues, there may be occasions when the police must be contacted.

**Cyber-Bullying**

Collingham College believes that all forms of bullying (including cyberbullying) should be handled as a community issue for the whole school. We take clear measures to prevent and tackle bullying among students as well as bullying of staff, whether by students, parents or colleagues.

"Cyber-bullying is an aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly over time against a victim who cannot easily defend him or herself." We recognise that the advent of cyber-bullying adds a new and worrying dimension to the problem of bullying as there no safe haven for the person being bullied. Unlike other forms of bullying, cyber-bullying can follow children and young people into their private spaces and outside school hours. Cyber-bullies can communicate their messages to a

wide audience with remarkable speed, and can often remain unidentifiable and unseen. ICT may be used to send threatening pictures or messages to others.

Seven categories of cyber-bullying have been identified:

- Text message bullying involves sending unwelcome texts that are threatening or cause discomfort;
- Picture/video-clip bullying via mobile phone cameras is used to make the person being bullied feel threatened or embarrassed, with images usually sent to other people;
- Phone-call bullying via mobile phone uses silent calls or abusive messages. Sometimes the bullied person's phone is stolen and used to harass others, who then think the phone owner is responsible. As with all mobile phone bullying, the perpetrators often disguise their numbers, sometimes using someone else's phone to avoid being identified;
- Email bullying uses email to send bullying or threatening messages, often using a pseudonym for anonymity or using someone else's name to pin the blame on them;
- Online grooming, Chat room and Social Networking Site abuse involves sending menacing or upsetting responses to children or young people;
- Bullying through Instant Messaging (IM) is an Internet-based form of bullying where children and young people are sent unpleasant messages as they conduct real-time conversations online;
- Bullying via websites includes the use of defamatory blogs (web logs), personal websites and online personal polling sites. There has also been a significant increase in social networking sites for young people, which can provide new opportunities for cyber-bullying.

Because of the anonymity that new communications technologies offer, anyone with a mobile phone or internet connection can be a target for cyber-bullying. Furthermore, bullies can reach much larger numbers within a peer group than they can with conventional bullying. Vindictive comments posted on a website, for instance, can be seen by a large audience, as can video clips sent by mobile phone. Although it leaves no visible scars, cyber-bullying of all types can be extremely destructive.

**Behaviour Policy**

The Behaviour Policy together with the Anti-bullying Policy contains up-to-date anti-bullying guidance, which should highlight relevant issues, such as cyber bullying. It should be recognised that all inappropriate behaviours will be taken seriously and dealt with in a similar way, whether committed on or offline. There are to be consistent expectations for appropriate behaviour in both the 'real' and 'cyber' world and this is to be reflected in all relevant policies.

**Support for staff on protecting their online reputation**

Our staff are in a position of trust. We have clear expectations that they will act in a professional manner at all times. Outlined below is some key advice for our staff which may help to protect their online reputation.

- Do not leave a computer or any other device logged in when you are away from your desk.
- Enabling a PIN or passcode is an important step to protect you from losing personal data and images (or having them copied and shared) from your mobile phone or device if it is lost, stolen, or accessed by students. Familiarise yourself with the privacy and security settings of the social media and apps you use and ensure they are kept up to date.
- It is a good idea to keep a check on your online presence – for example by typing your name into a search engine. If there is negative content online, it is much easier to deal with this as soon as it appears.
- Be aware that your reputation could be harmed by what others share about you online, such as friends tagging you in inappropriate posts, photographs, or videos.
- Consider your own conduct online; certain behaviour could breach your employment code of conduct.
- Discuss these same issues with close family, friends and colleagues, as you could become a target if they do not have security and privacy settings in place.
- Do not accept friend requests from students past or present. If you feel this is necessary, you should first seek guidance from a senior manager. Be aware that your social media friends may also be friends with students and their family members and therefore could read your post if you do not have appropriate privacy settings.
- Do not give out personal contact details – if students need to contact you with regard to homework or exams, always use your college contact details. On college trips, staff should have a Collingham mobile phone rather than having to rely on their own.

- Use your college email address for college business and personal email address for your private life; do not mix the two. This includes file sharing sites; for example Dropbox and YouTube.

**Advice on what to do if you're bullied**

We promote to our staff and students:

- You should never respond or retaliate to cyberbullying incidents. You should report incidents appropriately and seek support from your line manager or a senior member of staff.
- Save evidence of the abuse; take screen prints of messages or web pages and record the time and date.
- Where the perpetrator is known to be a current student or colleague, the majority of cases can be dealt with most effectively through the school's own mediation and disciplinary procedures.
- Where the perpetrator is known to be an adult, in nearly all cases, the first action should be for a senior staff member to invite the person to a meeting to address their concerns, and if they have a reasonable complaint, to make sure they know how to raise this appropriately. They can request that the person removes the offending comments.
- If they refuse, it should an organisational decision what to do next – either the college or you could report the matter to the social networking site if it breaches their terms, or seek guidance from the local authority, legal advisers or support from other agencies.
- If the comments are threatening or abusive, sexist, of a sexual nature or constitute a hate crime, you or a representative from the college may consider contacting the local police. Online harassment is a crime.

Employers have a duty to support staff and no-one should feel victimised in the workplace. Staff should seek support from the Senior Leadership Team. The Professional Online Safety Helpline is a free service for professionals and volunteers working with children and young people, delivered by the UK Safer Internet Centre. The helpline provides signposting, advice and mediation to resolve the e-safety issues which staff face, such as protecting professional identity, online harassment, or problems affecting young people; for example cyberbullying or sexting issues.

**Prevention of Extremism and Terrorism**

The Board of Directors, Principal and staff are fully aware of their duty of assessing the risk of our students being drawn into terrorism including support for terrorist ideology fundamental to which are extremist ideas. It is incumbent on us to be vigilant in ensuring that our students are safe from extremist and terrorist material when accessing the internet. Integral to our e-safety strategy is ensuring that appropriate filtering is in place. We take into account the Royal Borough of Kensington and Chelsea (LSCB) arrangement to fulfil Prevent duties as outlined in The Prevent duty, Departmental advice for schools and childcare providers (DfE 2015). This is achieved through the curriculum, our coverage of e-safety in the college's PSHE programme, being aware of student behavioural changes, being alert to any attempted external influences on the college and of, course through staff training. Prevent training for Leaders and Managers is carried out by the Designated Safeguarding Lead and Deputy Lead and all Personal Tutors. Prevent training for teachers is carried out by all staff.

---

**Legal Status:**

- Complies with Part 3 of The Education (Independent School Standards) (England) (Amendment) Regulations currently in force
- Based on guidance from the DfE, BECTA and CEOP along with
- The Education (Independent School Standards) (England) (Amendment) Regulations.
- Based on guidance from the DfE (2014) 'Cyberbullying: Advice for Principals and School staff 'and 'Advice for parents and carers on cyberbullying'.

**Applies to:**

- The whole college and all activities provided by the college, inclusive of those outside of the normal college hours;
- All staff (teaching and support staff), the Board of Directors and the proprietors of the college.

**Related documents:**
- Anti-bullying Policy
- Safeguarding - Child Protection Policy
- Behaviour Management Policy
- Online Teaching and Learning Policy

**Availability**
- This policy is made available to parents, staff and students in the following ways: via the college website and on request a copy may be obtained from the college office.

**Monitoring and Review:**
- This policy will be subject to continuous monitoring, refinement and audit by the Principal.
- The Principal will undertake a formal review of this policy for the purpose of monitoring and of the efficiency with which the related duties have been discharged, by no later than two years from the date shown below, or earlier if significant changes to the systems and arrangements take place, or if legislation, regulatory requirements or best practice guidelines so require.

Signed: Date: April 2022

Dr Sally Powell
Principal

Edward Browne and Robert Marsden
Board of Directors