CHELTENHAM COLLEGE CHELTENHAM PREP SCHOOL

Online Safety Policy

Reviewers: David Martin / Ester Leach
Approver: Anna Cutts
Reviewed: September 2025
Next Review: April 2026

1 Terms

For the purposes of clarity the following terms will be used throughout the policy:

- 'Cheltenham College' refers to Cheltenham College Senior School and Cheltenham College Preparatory School (including Cheltenham College Nursery School)
- 'College' refers to Cheltenham College Senior School
- 'Cheltenham Prep' refers to Cheltenham College Preparatory School
- 'Pre-Prep' refers to Cheltenham College Reception to Year 2, Nursery School / EYFS

Where policies are referred to, the following convention is used:

- CC denotes a whole-school policy
- P denotes a Prep policy
- C denotes a College policy

2 Introduction

It is the duty of Cheltenham College to ensure that every pupil in its care is safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods but also pose greater and more subtle risks to young people. Our pupils are therefore taught how to stay safe in the online environment and how to mitigate risks, including but not limited to, identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation. This includes education on emerging threats such as misinformation, disinformation, and the ethical use of generative AI. Pupils are also made aware of the risks associated with their digital footprint, and staff are supported with updated guidance on filtering, monitoring, and safeguarding in both physical and remote learning environments. We actively encourage open communication with families to ensure pupils are supported in making safe and informed choices online, both at school and at home.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. This policy acknowledges that online safety is as much about behaviour as it is about electronic security.

This policy, supported by the ICT Acceptable Use Policies for staff and pupils is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements. It is linked to the following school policies:

- Child Protection and Safeguarding Policy (CC)
- Child on Child Abuse Policy (CC)
- Staff Code of Conduct (CC)

- Pupil Behaviour Policy (C) and Prep Behaviour Policy (P)
- Anti-Bullying Policy (C) and (P)
- Pupil ICT Acceptable Use Policy (C)
- Pupil Acceptable Use Policy for younger pupils (P)
- Staff ICT Acceptable Use Policy (CC)
- Data Protection Policy (CC)

While digital technologies offer exciting and valuable opportunities both within and beyond the classroom, many online platforms and resources are not consistently monitored or regulated. It is essential that all users students, staff and visitors understand the wide range of potential risks associated with internet use and engage with these technologies responsibly and safely.

At Cheltenham College, we understand the responsibility to educate our pupils on online safety issues, teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom. We also understand the importance of involving pupils in discussions about online safety and listening to their fears and anxieties as well as their thoughts and ideas.

This is done through teachers, tutors and the Thrive! and Floreat Programmes, the schools' wellbeing programmes and includes the KCSiE areas of focus Content, Conduct, Contact Commerce:

- 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.
- Content: refers to the risk of children being exposed to illegal, inappropriate or harmful material online. This includes pornography, racism, misogyny, anti-Semitism, self-harm, suicide, radicalisation, extremism and violent content. Increasingly, children are also at risk from exposure to misinformation, disinformation including fake news, and conspiracy theories, which can distort their understanding of the world and influence their behaviour in harmful ways. Additionally, peer driven advertising and social listening, where content is tailored based on children's online activity, can subtly manipulate their choices and pose further safeguarding concerns.
- Conduct: personal online behaviour that increases the likelihood of, or causes digital self-harm or harm to others; for example, making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying). Sharing huge amounts of personal information (e.g. Snapmaps or games on Instagram)as well as password sharing.
- Commerce: risks such as online gambling, inappropriate advertising and risk of having brand ambassadors and peer to peer advertising, phishing and or financial scams.

3 Scope of this Policy

This policy applies to all members of the school community, including staff, pupils, parents and visitors, who have access to and are users of the school IT systems. In this policy 'staff' includes teaching and non-teaching staff, governors, and regular volunteers. 'Parents' includes pupils' carers and guardians. 'Visitors' includes anyone else who comes to the school, including occasional volunteers.

Both this policy and the ICT Acceptable Use Policies cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc); as well as any devices owned by pupils, staff, or visitors that are brought onto school premises (personal laptops, tablets, smart phones, etc).

4 Roles and responsibilities

4.1 Council

Council, the governing body of the school, is responsible for the approval of this policy and for reviewing its effectiveness. The governing body will review this policy at least annually. The Safeguarding Governor liaises with the school about online safety.

4.2 Heads and the Senior Leadership Teams

The Head of College and the Head of Prep hold overall responsibility for the safety and wellbeing of all members of the school community, which includes ensuring effective online safety practices.

To support this, they have delegated the day-to-day management of online safety to the Designated Safeguarding Leads (DSLs). The DSLs are further supported by the Filtering and Monitoring Committee, which provides guidance, monitoring, and strategic input to ensure a safe digital environment across the school.

In particular, the role of the Heads and the Senior Leadership team is to ensure that:

- Staff, in particular members of the DSL Team and the Filtering and Monitoring Committee are adequately trained about online safety as well as those who deliver online safety through the Thrive! And Floreat programs; and
- staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of online safety in connection to the school.

4.3 DSLs

The DSLs are responsible to the Heads for the day to day issues relating to online safety; ensuring this policy is upheld by all members of the school community and working with IT staff to achieve this, as well as keeping up to date on current online safety issues and guidance issued by relevant organisations, including the ISI, the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the Local Authority Safeguarding Children Board.

The DSL team is supported by the Online Safety Lead who in the College is also a DDSL.

4.4 Filtering and Monitoring Committee

To ensure a safe and secure digital environment for all members of the school community, the school has established a Filtering and Monitoring Committee. This committee plays a key role in overseeing the systems and processes that protect users from inappropriate or harmful online content.

The committee is responsible for:

- Reviewing and evaluating the effectiveness of the school's filtering and monitoring systems.
- Ensuring compliance with statutory guidance, including Keeping Children Safe in Education (KCSiE).
- Advising on improvements to digital safeguarding practices.
- Responding to incidents or concerns related to online safety and digital access.

By maintaining a proactive and informed approach, the Filtering and Monitoring Committee helps to ensure that digital technologies are used safely, responsibly, and in line with the school's safeguarding policies.

4.5 Online Safety Lead

As part of the Designated Safeguarding Lead (DSL) team, the school has appointed an Online Safety Lead to provide dedicated oversight and expertise in matters relating to digital safeguarding.

The Online Safety Lead is responsible for:

- Coordinating the school's approach to online safety, ensuring it aligns with statutory guidance and best practice.

- Monitoring emerging risks and trends in digital behaviour, online platforms, and technology use among pupils.
- Supporting staff and pupils with advice, training, and resources to promote safe and responsible use of digital technologies.
- Working closely with the Filtering and Monitoring Committee to ensure systems are effective and responsive to safeguarding needs.
- Responding to online safety incidents, concerns, or disclosures, and ensuring appropriate action is taken.
- Contributing to policy development, curriculum planning, and awareness campaigns related to online safety.

4.6 IT 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 computer systems and data and for training the school's teaching and administrative staff in the use of IT. They monitor the use of the internet and emails by staff, maintain content filters, and will report inappropriate usage to the DSLs. They ensure that suspected inappropriate use of the internet and emails by pupils are reported to the appropriate member of staff on duty and in accordance with the filtering and monitoring policy.

4.7 Teaching and support staff

All staff are required to accept and follow the Staff ICT Acceptable Use Policy before accessing the school's systems.

The Staff ICT Acceptable User Policy includes the requirement for promoting the online safety of pupils.

As with all issues of safety at this school, staff are encouraged to create a talking and listening culture in order to address any online safety issues which may arise in classrooms on a daily basis.

4.8 Pupils

Pupils are responsible for reading, understanding and adhering to the Pupil ICT Acceptable Use Policy including the reporting of concerns and for letting staff know if they see IT systems being misused.

4.9 Parents and carers

Cheltenham College believes that it is essential for parents to be fully involved with promoting online safety both in and outside of school. We regularly consult and discuss online safety with parents and seek to promote a wide understanding of the benefits and risks related to internet usage. The school will always contact parents if it has any concerns about pupils' behaviour in this area and likewise it actively encourages parents to feel able to share any concerns with the school

Parents and carers are responsible for endorsing the schools' ICT Pupil Acceptable Use Policies.

5 Education and training

5.1 Staff: awareness and training

Staff receive information on Cheltenham College's online safety, ICT Acceptable Use policies, and guidelines on the responsible use of generative AI tools as part of their induction.

All teaching staff receive regular updates and training on online safety, including the ethical and safe use of generative AI technologies, through INSET sessions and internal meetings. They are made aware of their individual responsibilities in safeguarding children within the context of online safety and emerging digital tools.

Staff working with children are responsible for promoting and modeling safe and responsible behavior, both in their classrooms and when using digital technologies, including generative AI. They must ensure adherence to school procedures that safeguard all members of the community.

Teaching staff are encouraged to integrate online safety and responsible generative AI use within their subject areas and cultivate an open culture where students can discuss digital issues as they arise. Staff should be familiar with procedures to follow in the event of technology misuse by any school community member; these are outlined in the Anti-Bullying and Child-on-Child Abuse Policy.

If any incident relating to online safety or inappropriate use of generative AI occurs, staff must complete a CPOMS entry promptly. These reports are directed to the school's Designated Safeguarding Leads (DSLs), who will take appropriate action and liaise as necessary.

5.2 Pupils: online safety in the curriculum

The use of IT and online resources is increasingly embedded across the curriculum, and we believe it is essential that pupils receive regular, meaningful guidance on how to stay safe online. We are committed to promoting online safety through a variety of approaches and continuously seek new opportunities to enhance pupils' understanding of the digital world. Their awareness and knowledge are regularly monitored and reinforced through both formal and informal learning experiences.

Online safety is taught across a range of curriculum areas, including dedicated IT lessons. In addition, pupils are educated about the risks associated with digital technologies beyond the school environment through our Thrive! and Floreat programmes, assemblies, and responsive discussions when relevant situations arise.

At age-appropriate levels, pupils are taught to understand their responsibilities for staying safe online and how to protect themselves and others. From Year 5, pupils receive specific education on recognising the signs of online sexual exploitation, stalking, and grooming, as well as understanding the associated risks and their responsibility to report any concerns involving themselves or their peers.

Pupils are encouraged to report any online safety concerns to the Designated Safeguarding Lead (DSL) or any trusted member of staff. From Year 9, pupils are also introduced to relevant legal frameworks surrounding internet use, including data protection, intellectual property, and the importance of respecting others' information and digital content.

Pupils are made aware of the impact of cyberbullying and are taught how to seek help if they are affected. They are encouraged to speak to their tutors, teachers, pastoral staff, the DSL, parents, peers, or any member of the school community if they experience difficulties online. Further guidance on this can be found in the school's Anti-Bullying Policy, which outlines both preventative measures and the procedures followed when incidents occur.

5.3 Parents

The school seeks to work closely with parents and guardians in promoting a culture of online safety. The 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 school.

The school recognises that not all parents and guardians may feel equipped to protect their child when they use electronic equipment at home. The school therefore arranges annual discussion events for parents when a specialist advises about online safety and the practical steps that parents can take to minimise the potential dangers to their children without curbing their natural enthusiasm and curiosity.

6 Policy Statements

6.1 Acceptable Use

Policies relating to the acceptable use of information and communication technology (ICT) shall be defined, approved by management, published and communicated to all staff, pupils and relevant parties.

Policies shall be differentiated and consistent, in that they recognise the age, role and the needs of users, particularly young people at different ages and stages within the schools whilst maintaining a common set of security and safety principles.

These policies shall be regularly reviewed in the light of current practice, legislation and changes in technology.

Acceptable use policies shall define a wide range of rules relating to both security and online safety including:

- Online and social media, including activities inside and outside school.
- Promoting online safety e.g. the supervision of pupil online safety of pupils by staff and the reporting of online safety incidents.
- Communication with pupils and parents by staff.
- The use of technology, including protecting devices and data.
- The use of digital and video images and online publishing.
- Fair use of shared resources.
- The retention of data and the protection of private information.
- Working or learning remotely.
- Personal use.
- Use of personal devices.
- Password Security.
- Incident Reporting.

6.2 Education and training

The education of pupils and staff on online safety shall be planned, developed, delivered and regularly reviewed for its effectiveness and impact.

6.3 Filtering and Monitoring

Access shall be blocked to illegal, unlawful terrorist and extremist online content via the school provided internet connectivity, in accordance with the IWF CAIC list.

Pupil access to online content via the school provided internet connectivity is blocked after 22:30 at night.

Filtering logs shall be regularly reviewed and breaches acted upon.

All users shall be aware of, and internet use shall be monitored for lawful purposes including, but not limited to, testing the security of the systems (e.g. penetration testing), detecting compromises to the security of the system (e.g. hacking), detecting misconduct (e.g. fraud), keeping children safe in education and preventing extremism (e.g. pupil online safety) and in support of criminal investigations.

Monitoring logs and alerts shall be reviewed and acted upon in a timely manner by a member of the DSL team. Pupils who are being monitored by the Welfare Management Team or are on the Pupils of Concern list would be considered a high priority pupil and acted upon accordingly. A search that triggers a high priority response would be entered on CPOMs unless the search is, after investigation, deemed safe.

Filtering and monitoring shall be implemented in a way that recognises the age, role and the changing needs of users, particularly young people at different ages and stages within the schools whilst providing the required access to content.

Changes to the filtering and monitoring systems shall be strictly controlled and implemented at times that minimise the risk of disruption to the school day. The continuing, effective filtering of illegal, unlawful terrorist and extremist online content must be verified as part of the change process, alongside adequate verification that the change itself was successfully implemented and did not adversely affect other filtering and monitoring system functionality.

The College's Filtering and Monitoring Committee meet termly to reassess the effectiveness of filtering and monitoring provisions.

6.4 Data and Security

A set of policies of procedures shall be maintained that ensures the school's ongoing compliance with data protection legislation and the effective protection of personal data.

All users shall be educated in these policies and procedures.

The school shall protect the security of its systems, data and users by implementing and maintaining a suite of information security controls that reduce information security risk to as low a level that is reasonably practical.

The school shall ensure the necessary resources for security and data protection are available and ensure data protection and security roles and responsibilities are defined and allocated.

7 Misuse

Cheltenham College will not tolerate illegal activities or activities that are inappropriate in a school context and will report illegal activity to the police and/or the Gloucestershire Safeguarding Children Partnership. If the school discovers that a child or young person is at risk as a consequence of online activity, it may seek assistance from Child Exploitation and Online Protection advisors.

Incidents of misuse or suspected misuse must be dealt with by staff in accordance with Cheltenham College's policies and procedures, in particular the Child Protection and Safeguarding Policy (CC).

The school 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 and Behaviour Policy.

8 Complaints

As with all issues of safety at Cheltenham College, if a member of staff, a pupil or a parent / carer has a complaint or concern relating to online safety, prompt action will be taken to deal with it. Complaints should be addressed to the Designated Safeguarding Leads at Prep and College in the first instance, who will liaise with relevant members of staff as needed and undertake an investigation where appropriate. Please see the Parents' Complaints Policy for further information.

Incidents of or concerns around online safety will be recorded and reported to the school's Designated Safeguarding Lead, in accordance with the school's Child Protection and Safeguarding Policy.