CHELTENHAM COLLEGE

CHELTENHAM PREP SCHOOL

E-Safety Policy

Reviewer: David Martin
Approver: Anna Cutts
Reviewed: April 2023
Next Review: April 2024

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, the risk of identity theft, bullying, harassment, grooming, stalking, abuse and radicalisation.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. This policy acknowledges that e-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 Behaviour Code of Conduct (CC)
- Behaviour Policy (CC)

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

Whilst exciting and beneficial both in and out of the context of education, much IT, particularly online resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

At Cheltenham College, we understand the responsibility to educate our pupils on e-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 e-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: etc

- 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: personal online behaviour that increases the likelihood of, or causes, harm; 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;
- Commerce: risks such as online gambling, inappropriate 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 e-safety.

4.2 Heads and the Senior Leadership Teams

The Heads are responsible for the safety of the members of the school community and this includes responsibility for e-safety. The Heads have delegated day-to-day responsibility to the Designated Safeguarding Leads (DSLs), who are supported by the E-Safety Group.

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

- Staff, in particular members of the e-safety group, are adequately trained about e-safety; and
- staff are aware of the school procedures and policies that should be followed in the event of the abuse or suspected breach of e-safety in connection to the school.

4.3 DSLs

The DSLs are responsible to the Headteachers for the day to day issues relating to e-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 e-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 DSLs are supported by the E-Safety Group.

4.4 E-Safety Group

The e-safety group is responsible for supporting the DSLs in discharging their e-safety responsibilities; keeping up-to-date on current e-safety issues; contributing to the development of e-safety-related policies, including filtering and monitoring policies; consulting stakeholders about the school's e-safety provision; providing training and advice for staff; mapping and reviewing the e-safety / digital literacy curricular provision, ensuring relevance, breadth and progressions and; monitoring improvement actions.

4.5 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.

4.6 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 e-safety issues which may arise in classrooms on a daily basis.

4.7 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.

4.8 Parents and carers

Cheltenham College believes that it is essential for parents to be fully involved with promoting e-safety both in and outside of school. We regularly consult and discuss e-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 e-Safety and ICT Acceptable Use policies as part of their induction.

All teaching staff receive regular information and training on e-safety issues in the form of INSET training and internal meeting time and are made aware of their individual responsibilities relating to the safeguarding of children within the context of e-safety.

All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school procedures.

When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's IT guidelines.

Teaching staff are encouraged to incorporate e-safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community; these are outlined in our Anti-Bullying and Child-on-Child Abuse Policy.

A CPOMS entry must be completed by staff as soon as possible if any incident relating to e-safety occurs. Such entries are provided directly to the schools' respective DSLs, who will liaise further as needed.

5.2 Pupils: e-Safety in the curriculum

IT and online resources are used increasingly across the curriculum. We believe it is essential for e-safety guidance to be given to pupils on a regular and meaningful basis. We continually look for new opportunities to promote e-safety and regularly monitor and assess our pupils' understanding of it.

The school provides opportunities to teach about e-safety within a range of curriculum areas and IT lessons. Educating pupils on the dangers of technologies that may be encountered outside school will also be carried out via Thrive! and Floreat programmes, by presentations in assemblies, as well as informally when opportunities arise.

At age-appropriate levels, pupils are taught about their e-safety responsibilities and to look after their own online safety.

From Year 5, pupils are taught in an age-appropriate manner about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across.

Pupils can report concerns to the respective DSL and any member of staff at the school.

From Year 9, pupils are also taught about relevant laws applicable to using the internet; such as data protection and intellectual property. Pupils are taught about respecting other people's information and images etc.

Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Anti-bullying Policy, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Pupils should approach their tutors, teachers, pastoral staff, the DSL as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

5.3 Parents

The school 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 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 e-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 ranges of rules relating to both security and e-safety including:

- Online and social media, including activities inside and outside school.
- Promoting e-safety e.g. the supervision of pupil online safety of pupils by staff and the reporting of e-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.

Commented [MP1]: I'm uncertain how this heading relates to the bullet points below?

6.2 Education and training

The education of pupils and staff on e-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 shall be blocked 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.

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.

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 Sanctions 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 e-safety prompt action will be taken to deal with it. Complaints should be addressed to the Designated Safeguarding Lead (Noll Jenkins at The Prep and Anna Cutts at College) in the first instance, who will liaise with relevant members of staff as needed and undertake an investigation where appropriate. Please see the Complaints Policy for further information.

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