Christ's College

Document Control	
Title	E-Safety Policy
Date	September 2024
Review	September 2025
Author	Mr Z Annan
Date adopted by Local Committee	N/A

At Christ's College as a community we understand the responsibility to educate our students on all e-safety issues; teaching them both appropriate behaviour and critical thinking skills to enable them to remain safe and legal when using the internet and related technologies.
Both this policy and the Acceptable Use Agreement (for all staff, governors, visitors and students) are inclusive of fixed and mobile internet technologies provided by the school.
Any visitors using their own devices within school, adhere to the schools Acceptable Use Agreement and this e-safety policy.
It is also important to recognise the constant and fast paced evolution of computing within our society as a whole. As a direct result of this, the E safety policy will be reviewed every 6 months and updated to adhere to trends in the online world.

Roles and Responsibilities

As e-safety is an important aspect of safeguarding within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are followed by all.
The named e-safety Lead's at Christ's College are;
-Mrs Shelley French, Vice Principal
-Mrs Jenny Fodor Assistant Principal & Designated Safeguarding Lead

If they are unavailable then any of the Deputy Designated Safeguarding Leads can be contacted these include the college principal, colleges leadership team and progress leaders.

Concerns can be reported to DSL@christscollege.surrey.sch.uk
This policy, supported by the school's acceptable use agreement, is to protect the interests and safety of the whole school community. It is linked to several other school policies including, Safeguarding, behaviour, and anti-bullying.
As a school we have a responsibility to keep our Staff, Governors and Parents up to date with changes in the online world. As a commitment to this we will have yearly CPD specific to E-Safety which all staff will complete.

E-Safety in The Curriculum

E-Safety will be promoted throughout the school in all subjects, especially as we continue to grow our Chromebook vision for the school.
Our School E-safety guidelines and the SMART rules will be prominently displayed around the school.
E-Safety will be taught as part of the rolling tutor time lessons and each year will look at different age specific topics.

Each year we participate in e-safety activities during Safer Internet Day. This will be in the form of PHSE sessions and Year Group Assemblies.
Christ's College recognises that E-safety travels across a broad number of subjects and has to be taught in respect of this.
Educating students on the dangers of technologies that maybe encountered outside school is done informally when opportunities arise and also part of the e-safety curriculum.
The teaching of e-safety will focus on giving the children the tools to keep them self-safe and recognise potential dangers online. By enabling the children with these skills not only are we safeguarding them but also helping them to support other friends or classmates. Cyber Bullying (social media Bullying) makes up over 75% of all Childline calls, this has been recognised by Christ's College and we take all cyber bullying very seriously For more information on Cyber Bullying please see the Anti-Bullying Policy.

Security, Data and Confidentiality

All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-safety Policy.

When accessing, amending and saving any data or information, relating to the school or students, school staff follow the guidelines set out in the General Data Protection Regulations 2021.

Managing the Internet

All internet activity within school is monitored and filtered through our Smoothwall system. Whenever any inappropriate use is detected, the E-Safety Coordinator is notified via automated email and the incident will be followed up in line with the school Acceptable Use Policy.
The school maintains students will have supervised access to Internet resources (where reasonable) through the school's digital devices. These include Net Support in the It rooms. If Internet research is set for homework, staff will remind students of their e-safety training. Parents are encouraged to support and supervise any further research.

Smart Watches/Devices

Smart watches that can freely access the internet or have a camera are not permitted in school.

Infrastructure

Our internet access is provided by TalkStraight and monitored by Schools Broadband.

Schools Broadband manage the administrative devices throughout school and curriculum access is managed by the school's Network Manager.

Staff and students are aware that they are monitored online, Schools Broadband is set to monitor the use of key words and topics and a list of these, alongside reports of children and staff accessing them is sent to the DSL daily.
The Network Manager has access to a Whitelist which can allow access for certain people to certain content for a short term. For example if in PE they are studying Drugs in sport, Drugs could be taken off the filter for those classes for the time they were studying. Only the network Manager has access to this Whitelist.

Mobile Technologies

Personal Mobile devices (including phones)

The school allows staff to bring in personal mobile phones and devices for their own use during designated times outside of the classroom. These are not to be used at any time whilst children are present. This does not include staff with specific work phones.
Children are not permitted to have their Mobile phone/ Electronic Device's on them while at school.

If caught with their Mobile phone/Electronic Device's on them they will have it confiscated and placed in the school safe until Friday (or when a responsible adult comes and collects it).
Mobile phones and smart watches can be authorised if they are for a medical condition. This request must be made to your child's Progress Leader. The school is not responsible for the loss, damage or theft of any personal mobile device or Electronic Device.

Managing email

The use of email within school is an essential means of communication for staff.
Students do have access to their school emails. They are not allowed to access personal email accounts while using school recourses Staff must use the school's approved email system for any school business. This includes Egress for secure and confidential emails.
Staff must inform (the e-safety co-ordinator/DSL (or DDSL's) if they receive an offensive or inappropriate e-mail.

Social Networking

The school does not permit the students to access their private accounts on social or gaming networks at any time during the school day or through school recourses.
The school also strongly discourages children from using age inappropriate social networking outside of school. This information can be provided by the E-safety Coordinator and is readily assessable for staff and parents. Should the staff be made aware of any such incidents or activities on these social networks, which have a direct effect on the children's Behaviour or attitudes within school, then the school reserves the right to take action regarding their accounts. This may include discussions with parents, information letters or reporting the child's access to the respective organisations/companies.

Safe Use of Images

Creation of videos and photographs

With the written consent of parents (on behalf of students) and staff, the school permits the appropriate taking of images by staff and students with school equipment.
All staff are aware of specific children (they have responsibility for) in school which do or do not have photograph permissions. If they do have permission, staff are aware of which platforms they can be used on, for example Twitter.
Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students, this includes field trips. School's own mobile devices must be used in this case.

Publishing students' images and work

All parents/carers will be asked to give permission to use their child's work/photos in publicity materials, on the school website or through the school's social media accounts.
This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue. Parents/ carers may withdraw or amend permission, in writing addressed to the school at any time.
Students' names will not be published alongside their image and vice versa on the school website and social media accounts.

Storage of Images

Images/ films of children are stored securely on the schools servers. Students do not have access to these pictures and all staff accounts are password protected.

Complaints

Complaints or concerns relating to e-safety should be made to the Principal.

If the complaint is about one of the mentioned people you have the right to go to the Chair of Local Committee.

Inappropriate material

All Staff/Students are aware of the procedures for reporting accidental access to inappropriate materials.

This must be immediately reported to the DSL, E-safety Coordinator or one of the DDSL's. Deliberate access to inappropriate materials will be dealt with by the DSL, E Safety Coordinator or another member of the safeguarding team.

Equal Opportunities

Students with additional needs (SEN)

The school endeavours to deliver a consistent whole school approach when it comes to parents and students and the schools' e-safety rules.

Staffs are aware that some students especially those with SEN will require further help and support in keeping themselves safe online.

Where a student has poor social understanding or SEN Needs. Internet activities are planned and well-managed for these children and young people; this will often include smaller group work and shorter more frequent sessions.