TRINITY
SCHOOL

Online Safety Policy

Trinity School (hereafter referred to as 'the school') recognises that students will have access to technologies that have both positive and negative potential. The school also recognises the enormous benefits to students of the internet as a means of academic research, for entertainment and for social interaction, and seeks to promote and encourage its effective use. The school is fully aware that online safety is directly related to safeguarding and takes seriously its responsibility to advise students, parents and staff of the significant dangers digital technologies can present when used inappropriately, whether this misuse be deliberate or unwitting.

This policy applies to all members of the school community (including staff, students, parents, visitors) who have access to and are users of school ICT systems, both in and out of the school and should be read in conjunction with the Staff, Student and Visitor Acceptable Use Policies, which offer clear guidance on the use of technology in the classroom and beyond for staff, students and visitors.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- content: being exposed to illegal, inappropriate or harmful material, 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; and
- commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams. Concerns about this type of risk to pupils, students or staff, should be reported to https://apwg.org/ the Anti-Phishing Working Group.

1. Oversight of online activity ~~Committees~~

a. Online Safety Committee:

The Online Safety Committee meets termly and consists of : the Director of Digital Strategy, the Deputy Head Pastoral (as Designated Safeguarding Lead), the Head of ICT and the Senior Deputy Head.

The committee:

- take day to day responsibility for online safety issues and have a leading role in establishing and reviewing the school's online safety policies and documents. Online safety incidents are recorded on MyConcern where they impact a singular or small number of students. These are managed via the pastoral team and reported to the Committee. Where an incident is of wider impact, members of the committee would directly oversee it's handling.
- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- arrange for the provision of training and advice for staff, parents and Governors (in liaison with the Head of Personal Development)
- are responsible for the online safety education of students. This is primarily done via Personal Development lessons where the Head of PD is managed by the DSL who sits on the committee.
- receive reports of online safety incidents and create a log of incidents to inform future online safety developments
- Oversee the filtering and monitoring of online activities.

More broadly, students, parents and staff should report any issues or concerns in relation to online activity or digital technology to any of the Online Safety Committee. If the matter relates to safeguarding, it should be reported to the Designated Safeguarding Lead (who is on this committee) or one of the Deputy Designated Safeguarding Leads. If none are available, the matter should be reported to a member of the Senior Management Team. **Anyone who teaches, coaches or supervises Trinity School students can make a direct referral to external safeguarding authorities at any time should they feel concerned about the welfare of a student.**

The contact details for the Local Authority Designated Officer are:

Local Authority Designated Officer (LADO):
Senior LADO: Steven Hall
LADO: Jane Parr
Business Support Officer: Karen Anns
Direct line: 020 8255 2889
lado@croydon.gov.uk

In Croydon, child protection referrals should be made to the 'Multi-Agency Safeguarding Hub' (MASH) and 'Early Help'
Professionals' consultation line **Tel: 0208 726 6464** Out of Hours **Tel: 0208 726 6400**

Referrals for students living outside the borough of Croydon will be made directly to the safeguarding team of the appropriate local authority.

Reports of concerns under the Prevent duty should be made to:
safercroydon@croydon.gov.uk

Further details about making referrals can be found in the Safeguarding and Child Protection policy.

b. Filtering and Monitoring:

In order to safeguard and promote the welfare of children and provide them with a safe learning environment, the governing body will do all that it reasonably can to limit children's exposure to the above risks from the School's IT system. This includes ensure the school has appropriate filtering and monitoring systems in place and that their effectiveness is regularly reviewed. The governors will ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place, manage them effectively and know how to escalate concerns when identified. To achieve this, the following should be considered: the number of and age range of the children, those who are potentially at greater risk of harm, how often they access the IT system and the proportionality of costs versus safeguarding risks.

As per KCSIE 2023, the appropriateness of filtering and monitoring systems is a matter for the school and is informed in part by the Prevent Duty. At Trinity, online activity is proactively filtered and monitored using commercial products: Sophos XG, Senso and Lightspead Alert and Filter. These products block staff and pupil access to inappropriate sites e.g., gambling and pornography and provide reports of any attempts by pupils and/or staff to access inappropriate sites. The list of sites blocked by these filters are routinely updated by the service providers.

As per the Department for Education filtering and monitoring standards, the school:

- Identifies and assigns roles and responsibilities to manage filtering and monitoring systems
- Reviews filtering and monitoring provision at least annually
- Blocks harmful and inappropriate content without unreasonably impacting teaching and learning
- Has effective monitoring strategies in place to meet safeguarding needs

The governing body will review these standards and discuss with IT staff and service providers what more needs to be done to support the school to meet this standard.

2. **Education and Training**

a. Students

Online Safety and best practice should be reinforced across the curriculum. The online safety curriculum is intended to be broad, relevant, current and to provide progression. The online safety curriculum is provided in the following ways:

- The online safety curriculum is explicitly included in the teaching of Computing and Personal Development (PD) and lesson content is regularly reviewed
- Key online safety messages are reinforced in assemblies
- Students are taught to be critically aware of the materials and content they access online and are guided to validate the accuracy of information
- Students are helped to understand the need for the Student Acceptable Use Policy and encouraged to adopt safe and responsible use both within and outside school.

- Students are helped to understand the benefits and risks associated with social media, online posting and messaging
- Staff should act as good role models in their use of digital technologies, the internet, and mobile devices
- The school recognises that 4G and 5G technology enables pupils to be online while not connected to the school's local area of wireless network. This access means some children, whilst at school, sexually harass their peers via their mobile and smart technology, share indecent images: consensually and non-consensually (often via large chat groups), and view and share pornography and other harmful content. The school takes the following measures to enhance the online safety of pupils:
    - Students in the Sixth Form may have mobile phones with them at school, but these must be switched off during lessons and other activities
    - Students in the Lower School and Middle School are required to keep their mobile telephones in their lockers during the day (including break and lunch) and must have permission from a member of staff before using them. Use will only be granted for vital calls e.g., to parents.
    - Educating students about the legal and personal consequences of sharing indecent images, sexual harassment, and harmful online content, including pornography, through the tutorial system, the Personal Development curriculum and the Sixth Form Diploma course.
- It is accepted that from time to time, for good educational reasons, students may need to research topics that would normally result in internet searches being blocked. In such a situation, staff can request IT Support to remove those sites from the filtered list for those students. Any request to do so should be submitted in writing to the ICT Manager, and obvious reasons for the need must be established and recorded.

b. Staff

- It is essential that all staff who are granted access to the Trinity School Network receive online safety training and understand their responsibilities, as outlined in this policy, as well as the School's Acceptable Use Policy, Staff Code of Conduct, Social Media Policy and Safeguarding and Child Protection Policy.
- The ICT Committee ensures that an audit of the online safety training needs of all staff with access to the network is carried out.
- All new staff are to receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Staff Acceptable Use Policy. This training is overseen by the Director of Digital Strategy.
- The Online Safety Officers will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- This Online Safety Policy and its updates will be available to staff in TEAMS and staff are required to acknowledge they have reviewed the above policies on an annual basis to the Senior Deputy Head.

c. Parents

Parents play an essential role in the education of their children and in the monitoring/ regulation of the children's on-line behaviours and interactions with digital technologies. The school will provide information about online safety to parents through seminars.

d. Governors

The Online Safety governor is the Chair of Welfare Sub-Committee, will be provided with opportunities to attend safety training sessions provided by professional organisations.

3. Roles and Responsibilities

Governors:

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This is carried out by the Welfare Committee, which will receive annual updates about online safety incidents. The role of the Online Safety Governor, includes:

- They are required to do all that they reasonably can to limit children's exposure to risks from the school's or college's IT system. This includes ensuring the school has appropriate filters and monitoring systems in place and regularly review their effectiveness.
- They should ensure that the leadership team and relevant staff have an awareness and understanding of the provisions in place and manage them effectively and know how to escalate concerns when identified.
- Governing bodies and proprietors should consider the age range of their children, the number of children, how often they access the IT system and the proportionality of costs verses safeguarding risks.
- Annually reviewing the quality of the school's provision of training for staff and information sessions for parents.
- Reporting to relevant Governors' meetings.
- Review feedback from the Online Safety Committee.

Headmaster and Senior Management Team:

- The Headmaster has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Officers, who report to the ICT Committee.
- The Headmaster, Designated Safeguarding Lead (DSL) and Deputy DSLs should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff.
- The Bursar shall ensure that the school's management of personal data is in line with statutory requirements (see Data Protection Policy for further details)
- The Senior Deputy Head and/or Pastoral Deputy Head will apprise the Senior Management Team will of any significant observations and findings made by the Online Safety Committee.

Senior Deputy Head:

- The Senior Deputy Head meets on a weekly basis with the Director of Digital Strategy to discuss all matters related to IT.
- The Senior Deputy Head hosts a termly meeting with the Director of Digital Strategy the Head of IT and Head of IM respectively.
- Alongside the Deputy Head Pastoral (DSL), the Senior Deputy Head monitors alerts from Senso (the school's IT monitoring and management system).

Director of Digital Strategy/Head of IT:

The Director of Digital Strategy and the Head of IT is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack
- that the school meets all online safety technical requirements as laid out in the Internet Security Information document
- that users may only access the school's networks and devices if properly authenticated and authorised
- that the filtering software remains current and fit for purpose
- that the use of the school's networks and devices is regularly monitored to ensure compliance with the Staff, Student and Visitor Acceptable Use Policies in order that any misuse or attempted misuse can be identified and reported to the appropriate person for investigation
- that filtering and monitoring software and systems are kept up to date.
- ensuring the appropriate level of security protection procedures in place, in order to safeguarding systems, staff and learners. These procedures are reviewed periodically to keep up with evolving cybercrime technologies, and to ensure that the Cyber Security Standards for schools are met.
- The ICT Manager is expected to keep up to date with online safety technical information in order to carry out their online safety role effectively and to inform and update others as relevant
- The Director of Digital Strategy will reinforce the importance of children being safe online with parents and carers via device training (e.g., what systems the school uses to filter and monitor online use. In addition, make parents and carers to aware of the sorts of activities that their children might be asked to do online).

Teaching and Support Staff:
Teaching and support staff are responsible for ensuring that:

- they have an up to date understanding of online safety matters and of the current Online Safety Policy and practices
- they have read and understood the Staff Acceptable Use Policy
- they report any suspected misuse or problem to the appropriate person for investigation
- all digital communications with other staff, students and parents are on a professional level and in accordance with the Staff Acceptable Use Policy
- they help students understand and follow the Online Safety and Student Acceptable Use Policy
- they help students acquire a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- Where possible share the sites/apps that they are asking students to access via Assignments.

If staff come across a website which they deem to be questionable or inappropriate within a school setting, please email ICTsupport@trinity.croydon.sch.uk.

See Appendix 1 for guidance on what to do in the event of **discovering content containing indecent images of children or criminally obscene adult content**

Designated and Deputy Designated Safeguarding Leads:

- The Deputy Head Pastoral, as the school's DSL:
    - Has responsibility for understanding the filtering and monitoring systems and processes in place.
    - Understands the expectations, applicable roles and responsibilities in relation to filtering and monitoring and includes this in safeguarding training which is regularly updated and shared with staff.
    - Oversees the school's child protection policy which includes how the school are using appropriate filtering and monitoring technology on school devices and school networks to safeguard children online.
- The DSL and DDSLs, in conjunction with the Director of Digital Strategy, are responsible for delivering appropriate safeguarding training to all staff at regular intervals and for ensuring that such training covers matters relating to online safety.
- The DSL and DDSLs are trained in online safety issues and will make staff aware of the potential for serious child protection and safeguarding issues to arise from:
    - sharing of personal data
    - access to illegal / inappropriate materials
    - inappropriate on-line contact with adults / strangers
    - potential or actual incidents of grooming
    - cyber-bullying.
    - Issues around copyright and plagiarism
    - Obsessive use of digital technologies
    - Social media concerns
    - Development of appropriate digital footprints

Students:

- are responsible for using the school's digital technology systems in accordance with the Student Acceptable Use Policy
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- will be expected to know and understand rules on the use of mobile devices and digital cameras. They should also know and understand rules on the taking/use of images and on cyber-bullying
- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the School's Online Safety Policy covers their actions out of school, if related to their membership of the school.

Parents

Parents play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. Parents are asked to support the school in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- access to the intranet and Parent Portal
- their children's personal devices in the school by their children.

Community Users

Community Users who access school systems as part of the wider school provision will be required to agree to an electronic Visitors' Acceptable Use Policy before being provided with access to school systems.

Author / Reviewer:	Mr Tuki Rounds (Senior Deputy Head)
Date of last review:	September 2023
Policy approved by:	Senior Management Team
Date of next Review:	September 2024

APPENDIX ONE

Discovery of content containing indecent images of children or criminally obscene adult content

The production and distribution of content that contains indecent images of children is an offence under the Protection of Children Act 1978 and the Sexual Offences Act 2003.

Being in possession of such content carries a penalty of up to five years in prison.

Making content, which includes downloading, storing and printing indecent images of children is an offence that carries a penalty of up to 10 years in prison.

If a user discovers content that contains indecent images of children, it is vital therefore that nothing is done that may lead to prosecution.

In the event of indecent images of children being discovered on a computer the following procedure should be followed:

1. **Lock the computer screen by pressing CTRL+ALT+DEL.**
2. **Do not print, copy, or email the content.**
3. **Do not look at any other content on the computer**
4. **Isolate the room where the PC is located. Lock a classroom if appropriate.**
5. **Inform the Headmaster and/or the Senior Deputy Head immediately.**

There is a conditional defence, agreed by the Crown Prosecution Service and the Association of Chief Police Officers, that allows designated IT professionals to access content containing indecent images of children for the purposes of forwarding them on to the Police and the Internet Watch Foundation (the approved body that deals with criminal content online, specifically child sex abuse images and criminally obscene adult content). At Trinity, the designated individuals are the Director of Digital Strategy (Mr Ryan van Graan) and the Network Manager (Mr Peter England). If indecent images of children are found, in consultation with the Headmaster, the Police, and the IWF, one of the designated individuals will access the content and retrieve evidence for the purpose of analysis and possible legal action. Nobody other than those named individuals above should ever attempt to access or distribute material of this nature.

If a user discovers content and there is uncertainty about whether it may be illegal or not, it is better to assume that it is and to follow the procedure above. The legal framework emphasises the importance of reporting illegal content in a timely manner. It is better to assume the worst and to allow a full review to occur swiftly, than leave content unexamined.

Where staff have concerns that school or private email accounts have been compromised and illegal content has been sent, or a link to such content provided, please inform the Headmaster of the Senior Deputy Head immediately. They will authorise a process involving the designated IT professionals to investigate any concern and where necessary, report it to the Police and the IWF.

Content of an illegal nature that is accessed, stored, made, or distributed outside of school using school equipment is subject to the same legal conditions outlined above. Should users detect illegal content on portable devices provided by the school the equipment should be locked and handed in to the IT Manager as soon as possible. Ideally, this should be within 12 hours of content being discovered. The Headmaster and/or the Senior Deputy Head should be telephoned and emailed immediately. Users should detail the nature of the content but not forward any content itself.

Where users discover content on the Trinity School Network that contains what may be deemed to be criminally obscene adult material the procedure above should be followed. Where staff accounts are found to have accessed or stored pornography via the Trinity School Network, that does not contain indecent images of children, this will be interpreted as a breach of the ICT Acceptable Usage Policy. Disciplinary procedures and dismissal may ensue consequently.

Further reading:
https://www.iwf.org.uk/resources/best-practice-guide
https://www.iwf.org.uk/resources/best-practice-guide/top-tips
https://www.iwf.org.uk/resources/best-practice-guide/frequently-asked-questions#2
https://www.iwf.org.uk/assets/media/hotline/CPS%20ACPO%20S46%20MoU%202014%202.pdf