TRINITY
SCHOOL

Online Safety Policy

Documentation for Regulatory Compliance: 7h

Trinity School (hereafter referred to as 'the School') recognises that pupils will have access to technologies that have both positive and negative potential. The School also recognises the enormous benefits to pupils 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 pupils, 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, pupils, 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, Pupil and Visitor Acceptable Use Policies, which offer clear guidance on the use of technology in the classroom and beyond for staff, pupils and visitors.

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

- content: being exposed to illegal, inappropriate or harmful material;
- contact: being subjected to harmful online interaction with other users; and
- conduct: personal online behaviour that increases the likelihood of, or causes, harm.

1. Committees

a. Online Safety Committee:

The Online Safety Committee shall consist of three Online Safety Officers: the Director of Digital Strategy, the Designated Safeguarding Lead and the Head of Personal Development. The committee shall meet termly and report to the ICT Committee.

The Online Safety Officers:

- 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
- 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 pupils

- receive reports of online safety incidents and create a log of incidents to inform future online safety developments

Pupil, parents and staff should report any issues or concerns in relation to online activity or digital technology to any of the Online Safety Officers. If the matter relates to safeguarding, it should be reported to the Designated Safeguarding Lead (who is an Online Safety Officer) 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 pupils is able to make a direct referral to external safeguarding authorities at any time should they feel concerned about the welfare of a pupil.**

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 'Single Point of Contact, which is made up of 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 pupils 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.

b. ICT Committee

The ICT Committee is composed of the Senior Deputy Head (Chair), Deputy Head Academic (Vice Chair), Bursar, IT Manager, Head of Information Management and Director of Digital Strategy. It shall meet monthly and reports, through the Senior Deputy Head, to the Headmaster and Senior Management Team.

Members of the ICT Committee will assist the Online Safety Officers with:

- the production, review and monitoring of the School's Online Safety Policy and Acceptable Use Policies (staff, pupil and visitors).
- the production, review and monitoring of the school filtering arrangements and requests for filtering changes
- mapping and reviewing the online safety curricular provision – ensuring relevance, breadth and progression
- monitoring incident logs (e.g. have any members of the community been exposed to illegal, inappropriate or harmful material; or has anyone been subjected to harmful online interactions with other users?)
- consulting stakeholders – including parents and pupils about the online safety provision of the School

- monitoring identified improvement actions

2. **Education and Training**

a. Pupils

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
- Pupils are taught to be critically aware of the materials and content they access online and are guided to validate the accuracy of information
- Pupils are helped to understand the need for the Pupil Acceptable Use Policy and encouraged to adopt safe and responsible use both within and outside school.
- Pupils 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
- It is accepted that from time to time, for good educational reasons, pupils 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 pupils. Any request to do so should be submitted in writing to the ICT Manager, and clear 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.
- Training will be arranged and overseen by the Head of Online Learning, and recorded as having taken place by the Senior Deputy Head
- The ICT Committee ensures that an audit of the online safety training needs of all staff with access to the network is carried out regularly.
- 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 Head of e-Learning.
- 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 presented to and discussed by staff in staff INSET.

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 John Crozier, Chair of Welfare Sub-Committee, will be provided with opportunities to attend safety training sessions provided by professional organisations.

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:

- Annually reviewing the quality of the School's provision of training for staff and information sessions for parents.
- Reporting to relevant Governors' meetings.
- Reviews the minutes of the ICT 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 Officers.

IT Manager:

The IT Manager 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, Pupil 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 monitoring software and systems are kept up to date.

The IT 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

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, pupils and parents are on a professional level and in accordance with the Staff Acceptable Use Policy
- they help pupils understand and follow the Online Safety and Pupil Acceptable Use Policy
- they help pupils acquire a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

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 DSL and DDSLs, in conjunction with the Head of e-Learning, 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

Pupils:

- are responsible for using the School's digital technology systems in accordance with the Pupil 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 T T Rounds (Senior Deputy Head)
Date of last review:	July 2019
Policy approved by:	Senior Management Team
Date of Approval:	September 2019
Date of next Review:	June 2020
Governor committee responsible for oversight:	Welfare Committee
Chairperson of Governor committee:	Jon Crozier
Date of review by committee:	21 January 2020

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 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 Head of e-Learning (Mr R van Graan) and the Network Manager (Mr H Ali). In the event that 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 or not 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 conent 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 possible dismissal may ensue as a consequence.

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