CATHEDRAL SCHOOLS TRUST | TRINITY ACADEMY

Online Safety (e-Safety) Policy

Name of policy	Online Safety (e-Safety) Policy
Date approved	September 2021
Date to be reviewed	September 2023

Introduction

In today's society, children, young people and adults interact with technologies such as mobile phones, games consoles and the Internet on a daily basis and experience a wide range of opportunities, attitudes and situations. The exchange of ideas, social interaction and learning opportunities involved are greatly beneficial to all, but can occasionally place children, young people and adults in danger. This policy outlines the steps Trinity Academy takes to mitigate the risks of online activity for all members of the school community.

Principles

E-Safety covers issues relating to children and young people as well as adults and their safe use of the internet, mobile phones and other electronic communications technologies, both in and out of school. It includes education for all members of the school community on risks and responsibilities and is part of the 'duty of care' which applies to everyone working with children. The risks associated with online activity are complex and varied – from breaches in personal data and identity theft to cyber bullying, blackmail and radicalisation.

The school will have robust processes in place to ensure the e-Safety of students, staff, volunteers and governors.

Roles and Responsibilities Surrounding E-Safety

Trinity Academy's Designated Safeguard Lead (DSL) acts as the designated e-Safety lead. His or her responsibilities include:

- Supporting the Headteacher in ensuring that staff understand the e-Safety Policy and that it is being implemented consistently throughout the school
- Working with the Headteacher, IT manager and other staff, as necessary, to address any e-safety issues or incidents
- Ensuring that e-safety incidents are logged onto CPOMS and dealt with appropriately
- Ensuring any incidents of cyberbullying are logged and dealt with in line with the School's Behaviour Policy and the Trust's Anti bullying Policy
- Organising, updating and delivering staff training on e-Safety
- Completing e-Safety audits at least annually (see appendix one)
- Liaising with other agencies and services as necessary (see appendix two for list of helpful contacts)
- Providing regular reports on e-Safety to the Headteacher and Governors.

The School's IT systems provider will support the School's commitment to safe online use by:

- Putting in place appropriate filtering and monitoring systems which are updated on a regular basis and keep students safe from potentially harmful and inappropriate content and contacts, including pornographic, terrorist and extremist material
- Ensuring that the school's IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly and fit for purpose
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any e-safety incidents and evidence of cyberbullying are promptly reported to the School's DSL and are appropriately dealt with.

All staff, including contractors and agency staff, and volunteers are responsible for reporting any e-Safety incidents to the School's DSL and to act in a responsible manner when using IT equipment – in accordance the Cathedral School Trust's (CST) Employment Manual.

The Headteacher is responsible for ensuring that staff understand this policy and that it is being implemented consistently throughout the school.

Teaching of E-Safety

Students will be taught about e-Safety as part of the curriculum through the School's PSHE Programme, assemblies and guest speaker events. This will include:

- How to use technology safely, respectfully and responsibly
- The acceptable and unacceptable behaviour surrounding online activity and, in particular, social media platforms
- How to report a range of concerns, both at school and to other organisations
- How changes in technology affect safety, including new ways to protect online privacy and identity
- The implications of digital footprints on everyday life and future careers
- The dangers of the uncritical acceptance of 'fake news' and other information that is intended to radicalise towards a particular extreme ideology

The school will also raise awareness of internet safety to parents through regular communications home, information via the school's website and Virtual Learning Environment (VLE) and through e-Safety seminars.

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyberbullying and the risks of online radicalisation. All staff will receive refresher training at least once a year as part of safeguarding training, along with regular updates as required.

Acceptable use of the Internet, Including using mobile devices, in school

Students use of personal devices

As outlined in the School's Behaviour Policy, students are not allowed to use mobile phones in school. If students bring mobile phones into school, it is at their own risk.

Staff using work devices outside of school

Staff members using a work device outside of school must not install any unauthorised software on the device and must not use the device in any way which would violate the school's terms of acceptable use, as set out in CST's Employment Manual.

Staff must ensure that their work device is secure and password protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside of school. Staff are only to use work devices outside of school solely for work activities.

Staff use of personal devices inside school

The following points relate to the use of personal devices by staff:

- Staff should avoid using their own personal phones or devices for contacting parents unless there is no alternative. In such cases, they should hide their number when calling
- Staff should not call students using their own personal phones or devices at any time and should instead use a school phone
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of students and will only use work-provided equipment for this purpose
- If a member of staff breaches the school policy then disciplinary action may be taken.

Use of Email

Below are points regarding the use of email:

- Students may only use approved email accounts for school purposes.
- Students must immediately tell a member of staff if they receive an offensive email
- Students must not reveal personal details of themselves or others in email communication, or arrange to meet anyone without specific permission from an adult
- Whole-class or group email addresses may be used by the school for communication outside of the school
- Staff will only use official school provided email accounts to communicate with students and parents or carers, as approved by the Senior Leadership Team
- Access in school to external personal email accounts may be blocked
- Email sent to external organisations should be written carefully, in the same way as a letter written on school headed paper would be

- The forwarding of chain messages is not permitted
- School will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff
- Staff should not use personal email accounts during school hours or for professional purposes.

Published content and the school website:

The following points relate to published content, including Trinity Academy's website:

- The contact details on the website should be the school address, email and telephone number. Staff or students' personal information will not be published
- Email addresses will be published carefully online, to avoid being harvested for spam
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

Publishing students' images and work

The following points relate to the publication of student images and work:

- Students' full names will not be used anywhere on the website, particularly in association with photographs
- Written permission from parents or carers will be obtained before images or videos of students are electronically published
- Students' work can only be published with their permission or the parents
- Written consent will be kept by the school where students' images are used for publicity purposes, until the image is no longer in use.
- Students and parents have the right to withdraw consent. In such circumstances, the school will make reasonable attempts to remove published material of the child in question.

Social Networking

The list below relates to the use of social networking and personal publishing within school:

- The school will attempt to control access to social media and social networking sites. This may include blocking of such sites using the school's firewall.
- Students will be advised never to give out personal details of any kind which may identify them and/ or their location. Examples would include real name, address, mobile or landline phone numbers, school attended, instant messaging and email addresses, full names of friends/family, specific interests and clubs etc.
- Staff wishing to use social media platforms with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will seek consent from the Senior Leadership Team before using social media platforms in the classroom if unsure
- Staff official blogs or wikis should be password protected and run with knowledge and with approval from the Senior Leadership Team. Members of staff should not run social network spaces for student use on a personal basis

- Students will be advised on security and privacy online and will be encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Students will be encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents or carers, particularly when concerning students' underage use of sites
- Staff personal use of social media will be discussed as part of staff induction and safe and professional behaviour is outlined in CST's Employment Manual.

Monitoring and Security of Information Access

Managing Filtering

The following points relate to the filtering of online material at Trinity Academy:

- The school's broadband access will include filtering appropriate to the age and maturity of students
- The school will ensure that the filtering process is continually reviewed
- The school will have a clear procedure for reporting breaches of filtering. All members of the school community (all staff and all students) will be aware of this procedure
- If staff or students discover unsuitable sites, the URL will be reported to the school's DSL who will then record the incident and escalate the concern as appropriate
- The school filtering system will block all sites on the Internet Watch Foundation (IWF) list
- Changes to the school's filtering will be risk assessed by staff with educational and technical experience prior to any changes and where appropriate with consent from the Senior Leadership Team
- The school Senior Leadership Team will ensure that regular (at least annual, in conjunction with the IT provider) checks are made to ensure that the filtering methods selected are effective.
- Any material that the school believes is illegal will be reported to appropriate agencies such as IWF, Bristol Police or CEOP by the DSL or another member of the safeguarding team.
- The school's access strategy will be designed by educators to suit the age and curriculum requirements of the students, with advice from network managers.

Information system security

The following points relate to the school's security of information:

- The security of the school information systems and users will be reviewed at least annually.
- Virus protection will be updated regularly

- Personal data sent over the Internet or taken off site will be encrypted
- Portable media may not be used without specific permission (from the IT provider) followed by an anti-virus / malware scan
- Unapproved software will not be allowed in work areas or attached to email
- The IT network manager will review system capacity regularly
- The use of user logins and passwords to access the school network will be enforced.

Managing VLE Access

The following points relate to the access to the school's VLE:

- SLT and staff will regularly monitor the usage of the VLE by students and staff in all areas, in particular message and communication tools and publishing facilities
- Students/staff will be advised about acceptable conduct and use when using the VLE
- Only members of the current students, parents or carers and staff will have access to the VLE
- All users will be mindful of copyright issues and will only upload appropriate content onto the VLE
- When staff and students leave the school their account or rights to specific school areas will be disabled or transferred to their new establishment
- Any concerns about content on the VLE may be recorded and dealt with in the following ways:
    - The user will be asked to remove any material deemed to be inappropriate or offensive
    - The material will be removed by the site administrator if the user does not comply
    - Access to the VLE for the user may be suspended
    - The user will need to discuss the issues with a member of SLT before reinstatement
    - A student's parent/carer may be informed
- A visitor may be invited onto the VLE by a member of the SLT. In this instance there may be an agreed focus or a limited time slot
- Students may require editorial approval from a member of staff. This may be given to the student to fulfil a specific aim and may have a limited time frame.

Managing emerging technologies

Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed. Students will be instructed about safe and appropriate use of merging technologies both on and off site in accordance with the School Communications Policy.

Authorising Internet access

The following points relate to the authorisation of internet access:

- The school will maintain a current record of all staff and students who are granted access to the school's electronic communications

- All staff will accept to the Trust's Acceptable Use Policy (see the Cathedral Schools Trust's Employment Manual) before using any school IT resources and confirm they will adhere to the Acceptable Use Policy on the VLE
- Students will apply for Internet access individually by agreeing to comply with the Acceptable Use Policy available on the VLE
- Parents will be asked to read the School Acceptable Use Policy for student access and discuss it with their child, where appropriate available on the VLE
- All visitors to the school site who require access to the schools network or internet access will be asked to read and sign an Acceptable Use Policy
- Parents will be informed that students will be provided with supervised internet access appropriate to their age and ability
- When considering access for vulnerable members of the school community (such as with children with special education needs) the school will make decisions based on the specific needs and understanding of the student(s)

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.

Responding to Issues of Concern

Handling of e-Safety Concerns

The following points relate to the handling of e-Safety concerns:

- The first and main priority is the safety and safeguarding of students and staff within our care
- Complaints about Internet misuse will be dealt with under the Trust's complaints procedure
- Any complaint about staff misuse will be referred to the Headteacher
- All e–Safety complaints and incidents will be recorded by the school, including any actions taken
- Students and parents will be informed of the complaints procedure
- Parents and students will need to work in partnership with the school to resolve issues
- All members of the school community will need to be aware of the importance of confidentiality and the need to follow the official school procedures for reporting concerns
- Discussions will be held with the local Police and/ or Children's Safeguarding Team to establish procedures for handling potentially illegal issues
- Any issues (including sanctions) will be dealt with according to the school's disciplinary, behaviour and child protection procedures
- All members of the school community will be reminded about safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos online which cause harm, distress or offence to any other members of the school community

Actions following e-Safety Concerns

The following actions may take place following concerns raised regarding e-safety:

- All members of the school community will be informed about the procedure for reporting e-Safety concerns (such as breaches of filtering, cyberbullying, illegal content etc)
- The DSL will record all reported incidents and actions taken in CPOMS
- The DSL will be informed of any e-Safety incidents involving child protection concerns, which will then be escalated appropriately
- The school will manage e-Safety incidents in accordance with the School's Behaviour Policy where appropriate
- The school will inform parents and carers of any incidents of concerns as and when required
- After any investigations are completed, the school will debrief, identify lessons learnt and implement any changes required
- Where there is cause for concern or fear that illegal activity has taken place or is taking place then the School will contact the Children's Safeguard Team or e-Safety officer and escalate the concern to the Police
- If the school is unsure how to proceed with any incidents of concern, then the incident may be escalated to the Area Children's Officer or the County e-Safety Officer
- If an incident of concern needs to be passed beyond the school then the concern will be escalated to the e-Safety officer to communicate to other schools in Bristol.

Managing Cyberbullying

In instances of suspected cyberbullying, the School will follow the procedures laid out in the Cathedral Schools Trust's Anti Bullying Policy. The definition of cyberbullying is clearly defined in the Anti Bullying Policy. Sanctions for those involved in cyberbullying may include:

- The perpetrator removing any material deemed to be inappropriate or defamatory or inflammatory content
- Contacting the service provider to remove content if the perpetrator refuses or is unable to delete content
- Suspending internet access at school for the perpetrator for a fixed or indefinite period of time
- Other sanctions in accordance to the School's Behaviour Policy and Exclusion Policy
- Contacting the Police if a criminal offence is suspected to have taken place.

<u>Policies Linked to the Online Safety Policy</u>

- Cathedral School Trust's Employment Manual
- Cathedral School Trust's Anti Bullying Policy
- Behaviour Policy
- Communications Policy
- CST Complaints Policy

Appendix One

School e-Safety Audit

This self-audit will be completed by the DSL in consultation with all stakeholders.

Has the school an e-Safety Policy that complies with education guidance?	Y/N
Date of latest update:	
Date of future review:	
The school e-safety policy was agreed by governors on:	
The policy is available for staff to access at:	
The policy is available for parents/carers to access at:	
The responsible member of the Senior Leadership Group is:	
The governor responsible for e-Safety is:	
The Designated Child Protection Coordinator is:	
The e-Safety Coordinator is:	
Were all stakeholders (e.g. Students, staff and parents/carers) consulted with when updating the school e-Safety Policy?	Y/N
Has up-to-date e-safety training been provided for all members of staff? (not only teaching staff)	Y/N
Do all members of staff sign an Acceptable Use Policy on appointment?	Y/N
Are all staff made aware of the schools expectation around safe and professional online behaviour?	Y/N
Is there a clear procedure for staff, Students and parents/carer to follow when responding to or reporting an e-Safety incident of concern?	Y/N
Have e-safety materials from Child Exploitation and Online Protection (CEOP), Childnet, and UK Council for Child Internet Safety (UKCCIS) been obtained?	Y/N
Is e-Safety training provided for all Students (appropriate to age and ability and across all Key Stages and curriculum areas)?	Y/N

Are e-safety rules displayed in all rooms where computers are used and expressed in a form that is accessible to all Students?	Y/N
Do parents/carers or Students sign an Acceptable Use Policy?	Y/N
Are staff, students, parents/carers and visitors aware that network and Internet use is closely monitored and individual usage can be traced?	Y/N
Has an ICT security audit been initiated ?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N
Is Internet access provided by an approved educational Internet service provider which complies with DfE requirements (e.g. KPSN)?	Y/N
Has the school filtering been designed to reflect educational objectives?	Y/N
Are members of staff with responsibility for managing filtering, network access monitoring systems adequately supervised by a member of the Senior Leadership Team (SLT)	Y/N
Does the school log and record all e-Safety incidents, including any action taken?	Y/N
Are the Governing Body and SLT monitoring and evaluating the school e-Safety policy and ethos on a regular basis?	Y/N

Appendix Two

e-Safety contacts and references

CEOP (Child Exploitation and Online Protection Centre): www.ceop.police.uk

Childline: www.childline.org.uk

Childnet: www.childnet.com

Click Clever Click Safe Campaign: http://clickcleverclicksafe.direct.gov.uk

Cybermentors: www.cybermentors.org.uk

Digizen: www.digizen.org.uk

Internet Watch Foundation (IWF): www.iwf.org.uk

Kidsmart: www.kidsmart.org.uk

Teach Today: http://en.teachtoday.eu

Think U Know website: www.thinkuknow.co.uk

Virtual Global Taskforce — Report Abuse: www.virtualglobaltaskforce.com

Additional Reading:

http://www.bristol.gov.uk/sites/default/files/documents/children_and_young_people/child_health_and_welfare/BSCB%20Annual%20Report%202012-13%20%5BFINAL%5D%20V1_08.pdf

https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis