Trinity Christian School

Nursery, Primary & Secondary

TRINITY

CHRISTIAN SCHOOL

E-Safety and Acceptable Use of ICT Policy

SLT Review Date:	November 2023
To be reviewed by SLT:	November 2024

Useful Contacts

Trinity Christian School Safeguarding Team Members emails, for Safeguarding reasons only:	
DSL Mrs Claire Bamford	c.bamford@trinityteachers.co.uk 07790301629
Deputy DSL/Head Teacher Mr Chris O'Gorman	c.ogorman@trinityteachers.co.uk 07757484038
Chair of Governors Mr Gareth Cottrell	chair@trinityschool.org.uk
E-Safety Governor Mr Sam Deakin	office@trinityschool.org.uk 0161 303 0674
Trinity School Office	office@trinityschool.org.uk 0161 303 0674
Online Safety Officer Mr Andrew Fisher	a.fisher@trinityteachers.co.uk
Network Manager Mr Jim Towell	office@trinityschool.org.uk 0161 303 0674

Outside Agencies:	
Police (non-emergency)	101
Darren Howarth Tameside Prevent Engagement Officer	darren.howarth@gmp.police.uk 0161 856 6345 / 07827979 13
Designated Officer (previously known as LADO) Tameside Safeguarding Children Partnership	tania.brown@tameside.gov.uk 0161 342 4398 / 07812 140 002 ladoreferrals@tameside.gov.uk 0161 342 4343
Internet and Filtering Software Smoothwall	smoothwall.com / enquiries@smoothwall.com 0800 047 8191
Anti-Phishing Working Group	http://apwg.org/report/phishing/
Child Exploitation and Online Protection (CEOP)	www.ceop.police.uk www.thinkuknow.co.uk
Childnet **NSPCC**	www.childnet.com www.nspcc.org.uk/onlinesafety
Childline	www.childline.org.uk
UK Safer Internet Centre	www.saferinternet.org.uk
Internet Watch Foundation	www.iwf.org.uk
Internet Matters	www.internetmatters.org
Net Aware	www.net-aware.org.uk

1.INTRODUCTION

This policy has carefully considered all relevant legislation and guidance including, but not limited to, the following:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2023) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2023) 'Keeping children safe in education 2023'
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2023) 'Generative artificial intelligence in education'

- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'

This Policy should be read in conjunction with the policies below:

- Data Protection
- Mobile phone and other electronic devices
- Safeguarding and Child Protection (including latest KCSIE)
- Behaviour Management
- Staff Code of Conduct
- Low Level Concern Policy
- Anti-Bullying Policy

2. PURPOSE

The purpose of this e-Safety policy is to:

- Safeguard and protect all members of the Trinity Christian School community online.
- Identify approaches to educate and raise awareness of e-Safety throughout the school community.
- Enable all staff to work safely and responsibly and to role model positive behaviour online.
- To manage professional standards and practice when using technology.
- Identify clear procedures to use when responding to e-Safety concerns.

3. RATIONALE

We believe that:

- The internet provides instant access to a wealth of up to the minute information and resources from across the world, which would not ordinarily be available.
- Virtual Learning Environments (VLEs) provide pupils with a platform for personalized and independent learning.
- Provides pupils with up-to-date learning and factual information from around the world.
- The internet and social networking sites enable pupils to research information outside of ordinary school hours and thus accelerate the potential for learning.
- Equips pupils with the necessary skills that they need for future employment and other life skills.

However, we also recognise:

- Pupils might inadvertently access content of an unsavoury, distressing or offensive nature on the internet or receive distasteful or offensive electronic messages.
- Pupils might receive unwanted or inappropriate emails from unknown senders or may be exposed to Cyber bullying.

- Pupils may be groomed online and make themselves susceptible to abuse – this includes students being made the victim of extremist or radicalisation content.

We believe that the advantages of the internet and electronic learning outweighs the risks involved, so long as users are made aware of the issues and concerns and receive guidance and education in choosing and adopting safe practices and behavior, within a safe environment.

The breadth of issues classified within E-Safety is considerable but can be categorised into FOUR areas of risk: **Content, Contact, Conduct and Commerce.**

Category	Possible danger
Content *'being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism' (KCSIE).*	Exposure to inappropriate content, including online pornography; ignoring age ratings in games (exposure to violence, often associated with racist language); substance abuse and "revenge porn". Lifestyle websites, for example pro-anorexia, self-harm or suicide sites. Hate sites. Exposure to radicalisation/terrorism sites. Content validation: how to check authenticity and accuracy of online content.
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' (KCSIE).*	Grooming. Cyberbullying Identity theft, including "frape" (hacking Facebook profiles) and sharing passwords.
Conduct *'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' (KCSIE).*	Privacy issues, including disclosure of personal information. Digital footprint and online reputation. Copyright (little care or consideration for intellectual property and ownership, such as music and film). Sexting (sending and receiving of personal or intimate messages)
Commerce *'risks such as online gambling, inappropriate advertising, phishing and or financial scams' (KCSIE).*	

Suspicious or obviously malicious emails can be reported to the Anti-Phishing Working Group http://apwg.org/report/phishing/

4. RESPONSIBILITIES

Trinity Christian School acknowledges that it is everybody's responsibility to Safeguard pupils and staff from any harm, as the school operates on a 'It could happen here' policy.

4.1. The Headteacher, SLT and the Governors will:

- ensure that e-Safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- have a named E-Safety Governor.
- ensure there are appropriate and up-to-date policies regarding e-Safety; including a Behaviour Policy, which covers acceptable use of technology.
- ensure that suitable and appropriate filtering and monitoring systems are in place and work with IT staff to monitor the safety and security of the school's systems and networks.
- ensure that e-Safety is embedded within a progressive curriculum, which enables all pupils to develop an age-appropriate understanding of e-Safety.
- support the DSL and Safeguarding team by ensuring they have sufficient time and resources to fulfill their e-Safety responsibilities.
- ensure there are robust reporting channels for the community to access regarding e-Safety concerns, including internal, local and national support.
- ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- audit and evaluate e-Safety practice to identify strengths and areas for improvement.
- regularly monitor online safety incident logs.
- regularly monitor filters.
- appoint a named member of staff to maintain and monitor the school web-page.
- appoint a named member of staff to maintain and monitor the school facebook page.

4.2. The DSL will:

- act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.
- work alongside the national and local recommendations and requirements to ensure e-Safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- ensure that suitable and appropriate filtering and monitoring systems are in place and work with IT staff to monitor the safety and security of the school's systems and networks.
- ensure all members of staff receive regular, up-to-date and appropriate e-Safety training, including practice, procedures, expectations, roles and responsibilities.
- access regular and appropriate training and support to ensure they understand the unique risks associated with e-Safety and have the relevant and up to date knowledge required to keep pupils safe online.
- access regular and appropriate training and support to ensure they recognise the additional risks that pupils with SEN and disabilities (SEND) face online.

- keep up-to-date with current research, legislation and trends regarding e-Safety and communicate this with the community, as appropriate.
- ensure that e-Safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- maintain records of e-Safety concerns, as well as actions taken, as part of the school's safeguarding recording mechanisms.
- monitor e-Safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- report e-Safety concerns, as appropriate, to the Headteacher, SLT and Governing Body.
- work with the SLT and IT staff to review and update e-Safety policies on a regular basis (at least annually).
- meet termly with the governor with a lead responsibility for safeguarding.
- meet annually with the governor with a lead responsibility for online safety.
- work with the OSO to produce effective risk assessments in relation to BYOD (Bring Your Own Devices).

4.3. The Online Safety Officer will:

- ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- work with the DSL and SLT to provide training and advice is provided for staff.
- act as the main liaison with the school Network Manager, and the Web Filtering and Monitoring agency.
- receive reports of online safety incidents and create a log of incidents to inform future online safety developments.
- meet termly with the DSL to discuss current issues, review incident logs and filtering / change control logs.
- 'review' half-termly the effectiveness of the web filtering and monitoring systems.
- 'review' annually along with the DSL the effectiveness of the web filtering and monitoring systems.
- ensure that the most up-to-date Internet and filtering software (Smoothwall) is installed at Trinity Christian School.
- keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- update relevant software and ensure that only the IT staff can install software to prevent viruses from being accidentally installed on machines.
- work with the DSL and SLT to review and update e-Safety policies on a regular basis (at least annually).
- support the DSL and SLT in ensuring that parents are kept up to date on issues of e-safety.
- work with the DSL to produce effective risk assessments in relation to BYOD (Bring Your Own Devices).

4.4. The Network Manager will:

- ensure that the *school's* technical infrastructure is secure and is not open to misuse or malicious attack.
- ensure that the *school* meets required online safety technical requirements and any Local Authority or other relevant body online Safety Policy / guidance that may apply.
- secure that users may only access the networks and devices through a properly enforced password protection policy.

- keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant.
- ensure that the use of the network / Internet / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher and Online Safety Officer for investigation.
- maintain the school's Antivirus software installed and keep it up to date.
- work with the OSO to make sure that monitoring software / systems are implemented and updated as agreed.
- establish and maintain a system to back up Staff and pupils' Network Data daily.

4.5. Staff:

It is the responsibility of all members of staff to:

- make sure they have an up-to-date awareness of online safety matters and of the current Online Safety Policy and practices.
- read, and understand the e-safety policy.
- report any suspected misuse or problem to the Headteacher, DSL or Online Safety Officer for investigation.
- ensure that all digital communications with students / pupils / parents / carers should be on a professional level.
- embed all online safety issues within all aspects of the curriculum and other activities.
- help pupils to understand and follow the Online Safety Policy and acceptable use policies.
- assist pupils to have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.
- monitor the use of digital technologies, mobile devices, cameras etc in lessons and other school activities (where allowed) and implement current policies and risk assessments in regard to these devices.
- guide pupils within lessons, where internet use is pre-planned, to sites checked as suitable for their use and to be aware of the processes that are in place for dealing with any unsuitable material that is found in internet searches.
- appropriately display and communicate the rules and procedures for safe internet use.
- seek permission from the OSO or Network Manager prior to installing any Software.
- liaise with the OSO when research may require the web filtering to be altered to allow for specific research terms.
- ensure that electronic devices (PC's, laptops, tablets etc) must never be left logged on and left unattended. If machines are to be left unattended, they should be locked (Ctrl+alt+del followed by lock computer) or logged off.
- ensure that electronic devices are logged off after use and shut down at the end of the school day.
- comply with the rules of the school's internet use that it must only be accessed for professional or educational purposes (staff must not use the internet to access social networking sites, shopping sites or for other uses in connection with their private lives).
- return laptops back to Room 2/6 when not in use.
- use the school network or Google drive for storing files. Memory sticks are not used as a primary place of storage.
- consult the parental permissions for photographing pupils especially when the photos are to be used on the school web-page or Facebook page.

4.6. Pupils:
It is the responsibility of all pupils to:

- access the network using their own logons and passwords. These must never be disclosed or shared.
- respect confidentiality and attempts should never be made to access another person's individual folder on the network without permission to do so.
- ensure that electronic devices are never left logged on and left unattended. If machines are to be left unattended, they should be locked (Ctrl+alt+del followed by lock computer) or logged off.
- ensure that electronic devices are logged off after use and shut down at the end of school if they have been using a device at the end of the day.
- sign an E Safety User Agreement, when in Years 7-11, before being given access to the internet.
- report accidental access to inappropriate sites (racist, abusive, pornographic or otherwise) to the teacher and a note will be taken of the offending site and blocked by the OSO.
- never disclose personal details about themselves or others online.
- **to accept and understand that bullying, harassment or any kind of Cyber abuse will not be tolerated. Sanctions will be applied to the user who breaks this code (regardless of if the offence occurs outside of school hours or off school site- please refer to the Behaviour Management Policy).**
- to use the school systems, such as google classroom, safely and appropriately.
- to report any instances, whether it is about them or another pupil, of cyber bullying to the DSL.
- to seek permission from the OSO before downloading any files.
- to ask for permission from a teacher before using an electronic device in school and must be supervised at all times while using the internet.

4.7. Parents and Carers:
All parents and carers are required to:

- to sign the E-Safety consent form before the school can allow pupils to use the Internet.
- to support the school's e-Safety approaches by discussing e-Safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- to role model safe and appropriate use of technology and social media.
- to identify changes in behaviour that could indicate that their child is at risk of harm online.
- to seek help and support from the school, or other appropriate agencies, if they or their child encounter risk or concerns online.
- to use school systems, such as Studybugs and google classroom, safely and appropriately.
- to take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.
- to read any e-safety guidance given by school.

5. EDUCATION

5.1. All pupils:
Trinity Christian School will establish and embed an effective e-Safety curriculum throughout the school to raise awareness and to promote safe and responsible internet use amongst pupils by:

- ensuring education regarding safe and responsible use precedes internet access.
- including e-Safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education as well as Computing lessons.
- reinforcing e-Safety messages whenever technology or the internet is in use in all lessons.
- educating pupils in the effective use of the internet to research.
- teaching pupils to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Trinity Christian School will support pupils to read and understand the E-safety and Safeguarding policies in a way which suits their age and ability by:

- displaying acceptable use posters in all rooms with internet access.
- informing pupils that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- informing parents and carers that network use will be monitored for safety and security purposes and in accordance with legislation.
- rewarding positive use of technology.

5.2. Vulnerable Pupils:
Trinity Christian School recognises that some pupils are more vulnerable online due to a range of factors. This may include, but is not limited to children in care (LAC), children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

Trinity Christian School will ensure that differentiated and ability appropriate e-Safety education and support is provided to more vulnerable pupils. The DSL will offer support and guidance where necessary.

5.3. Staff:
Trinity Christian School will:

- provide and discuss the E-Safety policy and procedures with all members of staff as part of induction.
- provide up-to-date and appropriate e-Safety training for all staff on a regular basis, with at least annual Safeguarding updates - this will cover the potential e-safety risks posed to pupils (Content, Contact and Conduct) as well as our professional practice expectations
- make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.
- highlight useful educational resources and tools which staff should use, according to the age and ability of the pupils.
- ensure all members of staff are aware of the procedures to follow regarding e-Safety concerns affecting pupils, colleagues or other members of the community.

5.4. Parents / Carers:
Trinity Christian School recognises that parents/carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.

We will build a partnership approach to e-Safety with parents/carers by:

- providing information and guidance on e-Safety in a variety of formats.
- drawing their attention to the e-Safety Policy and expectations in the parent handbook and on the school's website.
- requesting that they read this policy prior to signing e-safety consent form, and discuss the implications with their child/ren.

6. REDUCING ONLINE RISKS

Trinity Christian School recognises that the internet is a constantly changing environment with new applications, devices, websites and material emerging at a rapid pace.

We will:

- regularly review the methods used to identify, assess and minimise online risks.
- examine new technologies for educational benefit and undertake appropriate risk assessments before use in the school is permitted.
- ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.

Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via the school's computers or devices.
All members of the community are made aware of the school's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the community. This is clearly outlined throughout this policy and highlighted through a variety of education approaches.

7. SAFER USE OF TECHNOLOGY

7.1. Classroom Usage:
Trinity Christian School uses a wide range of technology. This includes access to:

- Computers, laptops and other digital devices
- Internet which may include search engines and educational websites
- Manga High/Studybugs/google classroom
- Email
- Digital cameras, web cams

All school owned devices will be used in accordance with School policies and with appropriate safety and security measures in place:

- Members of staff will always evaluate websites, tools and applications fully before use in the classroom or recommending for use at home.
- We will use age-appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.
- We will ensure that the use of internet-derived materials, by staff and pupils, complies with copyright law and acknowledge the source of information.
- Supervision of pupils, when using technology, will be appropriate to their age and ability.

- If a staff member is concerned about anything pupils raise during online safety lessons and activities, or at any other time, they will make a report in line with the Safeguarding and Child Protection Policy.
- Members of staff are aware that they cannot rely on the web filtering and monitoring system for Safeguarding, and that their vigilance and pro-activity is essential.

7.2. Filtering and Monitoring:

- The Governors, working with the DSL and OSO, will ensure the school's network has appropriate filters and monitoring systems in place and that it is meeting the DfE's 'Filtering and monitoring standards for schools and colleges'.
- The decisions regarding the level of web filtering and monitoring have been informed through risk assessments.
- The OSO will maintain a written record of users who are granted access to our devices and systems.
- All staff and pupils will read and sign an acceptable use policy before being given access to our computer system, IT resources or internet.
- Levels of Internet access and supervision will vary according to the pupil's age and experience. Older pupils, as part of a supervised project, might need to access specific adult materials - for instance a course text or set novel might include references to sexuality - while teachers may need to research areas including drugs, medical conditions, bullying, racism or harassment. In such cases, the restrictions imposed by the school's filtering system may be removed temporarily while the user accesses the material under close supervision. In order to do this, subject teachers will liaise with the OSO prior to the start of the lesson. The OSO and DSL will conduct a risk assessment to assess the appropriateness of the request.
- All reviews and changes to the filtering will be recorded.
- Staff and pupils who discover that an unsuitable site is accessible must report this to the OSO or DSL.
- The OSO will manage the configuration of the filtering system to ensure that it is appropriate, effective and reasonable.
- The DSL or OSO will report any online material it believes to be illegal to the appropriate agencies.
- Smoothwall web filtering blocks sites which can be categorised as pornography, racial hatred, extremism, gaming and sites of an illegal nature. The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- If pupils discover unsuitable sites, they will be required to report their concern to a member of staff. The member of staff will report the concern (including the URL of the site if possible) to the DSL and /or the OSO and the breach will be recorded and escalated as appropriate.
- Parents/carers will be informed of filtering breaches involving their child.
- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Greater Manchester Police or Child Exploitation and Online Protection command (CEOP).
- The OSO will appropriately monitor internet use on all school owned or provided internet enabled devices. If a concern is identified the DSL will be informed as appropriate.
- All users will be informed that use of the systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

7.3. Passwords:

- All members of staff will have their own unique username and private passwords to access the School's system and are required to keep their password private.
- From Year 7, all pupils are provided with their own unique username and private passwords to access the School's system and pupils are responsible for keeping their password private. Logging into another pupil's account is in breach of their E-Safety User Agreement and will result in the appropriate sanction as stated in the Behaviour Policy.
- Users will inform the OSO if they forget their login details, who will arrange for the user to access the systems under different login details.

7.4. Managing Email:

- Access to the School's email systems will always take place in accordance with data protection legislation and in line with other policies including (but not limited to) the: Behaviour Policy, Safeguarding and Child Protection Policy, and Data Protection Policy.
- The forwarding of any chain messages/emails is not permitted.
- All staff are provided with their own personal work email.
- All pupils from Year 7 are provided with their own personal school email for educational purposes and so that they can access google classroom.
- Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email such as through egress.
- School email addresses and other official contact details will not be used for setting up personal social media accounts or for any personal correspondence.
- Staff and pupils will immediately tell the DSL and/or OSO if they receive offensive communication, and this will be recorded on our safeguarding database.

8. SOCIAL MEDIA

Trinity Christian School acknowledges that in today's world, many people engage in social media for purposes such as information/news, communication, friendship, gaming and learning. The term social media may include (but is not limited to): *blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.*

The use of social media accounts on school devices is not permitted, other than for designated members of staff to up-date the School's website and Facebook page. The Behaviour Policy, the Staff Code of Conduct and the Staff Disciplinary procedures will be followed for pupils and staff found in breach of this.

In their free time, all members of Trinity Christian School are expected to engage in social media in a positive, safe and responsible manner. They are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.

Concerns regarding the online conduct of any member of staff or pupil should be reported to the DSL and will be managed in accordance with our Safeguarding and Child Protection Policy, Low Level Concerns Policy, and Behaviour Policy.

8.1. Staff:

The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.

Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our Code of Conduct.

All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the school.

Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

All members of staff are advised to safeguard themselves and their privacy when using social media sites.

All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with our policies and the wider professional and legal framework.

Information and content that staff members have access to as part of their employment, including photos and personal information about pupils and their family members or colleagues will not be shared or discussed on social media sites.

Members of staff will notify the DSL and/or the Headteacher immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with pupils and parents/carers:

- All members of staff are advised not to communicate with or add as 'friends' any current or past pupils or their family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this, will be discussed with the DSL and/or the Headteacher.
- Staff will not use personal social media accounts to contact pupils or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the DSL and/or the Headteacher.
- Any communication from pupils and parents received on personal social media accounts will be reported to the DSL and/or The Headteacher.

8.2. Pupils' Personal Use of Social Media:

- Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age appropriate sites and resources.
- Any concerns regarding a pupil's use of social media will be dealt with in accordance with existing policies, including Anti-Bullying, Behaviour and Safeguarding and Child Protection. Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.
- Where appropriate, advice and information will be shared with Trinity parents regarding the appropriate use of social media.

Pupils will be advised:
- To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location
- To only approve and invite known friends on social media sites and to deny access to others by making profiles private
- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present
- To use safe passwords
- To use social media sites which are appropriate for their age and abilities
- How to block and report unwanted communications
- How to report concerns both within the setting and externally

8.3. School's social media:
Trinity Christian School does have a Facebook page. This is primarily used as an additional way to share events and news with parents. The Head Teacher and DSL have appointed one member of staff to up-date and maintain the page. This member of staff will:

- not engage with any direct or private messaging with current pupils, parents/carers
- inform the DSL and /or OSO of any concerns, such as criticism, inappropriate content or contact from pupils.

We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Members of staff who follow and/or like our official social media channels will be advised to use dedicated professional accounts, where possible, to avoid blurring professional boundaries.

9. TAKING PHOTOS

Trinity Christian School acknowledges the importance of taking photos throughout the school day and particularly at school events. However:

- Staff and pupils should use the designated school camera located in the School Office.
- Staff should download images on the day that images are taken or ask the Office Staff to do so.
- Staff are *not permitted* to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However, with the express permission of the Headteacher or DSL, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.
- Parents must not take photos of other people's children and should never upload photos on social media sites (e.g. Facebook) without permission from the child's parents.
- Photographs of pupils may only be taken if permission has been granted by the parent/carer at the start of the school year.

For more information, please refer to the Mobile Phone and Electronic Devices Policy.

10. USE OF MOBILE PHONES

Staff should not be using their own mobile phones when in supervision of pupils, except in an emergency situation such as a medical emergency. Exemptions to this, can only be granted by the Head Teacher or DSL and must be recorded on the School's E-Safety Risk Assessment.

Pupils are banned from using mobile phones in school hours. All pupils must turn their phones off on arrival and hand them in to the Form teacher during morning registration. The phone will be returned during final afternoon registration. However, there are certain exceptions to this rule and these must be authorized by the Head Teacher or DSL, and recorded on the School's E-Safety Risk Assessment.

For more information, please refer to the Mobile Phone and Electronic Devices Policy.

11. WIRELESS NETWORK

Trinity Christian School offers a wireless network. To maintain e-safety this is encrypted and protected by a password. This password is only given to staff on a need to know basis and is **NEVER SHARED WITH PUPILS OR VISITORS TO THE SCHOOL** (including parents).

12. RESPONDING TO E-SAFETY INCIDENTS AND CONCERNS

All members of the school will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.

All members of the school must respect confidentiality and the need to follow the official procedures for reporting concerns. Pupils, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.

We require staff, parents / carers and pupils to work in partnership to resolve online safety issues. After any investigations are completed, the DSL will debrief, identify lessons learnt and implement any policy or curriculum changes as required.

If we are unsure how to proceed with an incident or concern, the DSL will seek advice from the Tameside Safeguarding Children Partnership.

Where there is suspicion that illegal activity has taken place, the DSL will contact Tameside's Designated Officer, or Tameside Safeguarding Children Partnership or Greater Manchester Police using 101, or 999 if there is immediate danger or risk of harm.

If an incident or concern needs to be passed beyond our community (for example if other local schools are involved or the public may be at risk), the DSL will speak with Greater Manchester Police and/or the Tameside Safeguarding Children Partnership first to ensure that potential investigations are not compromised.

12.1. Concerns about Pupils' Welfare:

- The DSL will be informed of any online safety incidents involving Safeguarding or Child Protection concerns via completion of a Safeguarding form.

- The DSL will record these issues in line with our Safeguarding and Child Protection policy.
- The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the Tameside Safeguarding Children Partnership thresholds and procedures.
- The DSL will inform parents / carers of online safety incidents or concerns involving their child, as and when required.

12.2. Staff Misuse:

- Any complaint about staff misuse will be referred to the DSL.
- Any allegations regarding a member of staff's online conduct will be discussed with the Local Authority Designated Officer (LADO).
- Appropriate action will be taken in accordance with our Safeguarding and Child Protection Policy for Managing Allegations against Staff.

12.3. Online Sexual Violence and Sexual Harassment Between Children:

- The school recognises that sexual violence and sexual harassment between children can take place online.
- Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation. Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our Behaviour, Safeguarding and Child Protection and Anti-bullying Policies.
- The school recognises that the internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- The school also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- The school will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE curriculum.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.

If made aware of online sexual violence and sexual harassment, staff will:

- Immediately notify the DSL and act in accordance with our Behaviour, Safeguarding and Child Protection and Anti-bullying Policies.
- If content is contained on pupils' electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
- Provide the necessary safeguards and support for all pupils involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
- Implement appropriate sanctions in accordance with our behaviour policy.
- Inform parents / carers, if appropriate, about the incident and how it is being managed.
- If appropriate, make a referral to partner agencies, such as Children's Social Services and/or the Police.

- If the concern involves children and young people at a different educational setting, work in
- partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
- If a criminal offence has been committed, the DSL will discuss this with Greater Manchester Police first to ensure that investigations are not compromised.
- Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

12.4. Youth Produced Sexual Imagery:
The school recognises youth produced sexual imagery (known as "sexting") as a safeguarding issue. As a school we will:

- ensure that all concerns are reported to and dealt with by the DSL.
- follow the advice as set out in the non-statutory UK Council for Child Internet Safety (UKCCIS) guidance: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis
- follow the advice of Tameside Safeguarding Children Partnership.
- follow the advice as set out by the NSPCC https://learning.nspcc.org.uk/research-resources/briefings/sexting-advice-professionals
- ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of 'sexting' by implementing preventative approaches, via a range of age and ability appropriate educational methods.
- ensure that all members of the community are aware of sources of support regarding youth produced sexual imagery.
- respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using school provided or personal equipment.

We will not:

- view any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so - If it is deemed necessary, the image will only be viewed by the DSL and their justification for viewing the image will be clearly documented.
- send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request pupils to do so.

If made aware of an incident involving the creation or distribution of youth produced sexual imagery, we will:

- act in accordance with our safeguarding and child protection policies and the relevant Tameside Safeguarding Children Partnership Board's procedures.
- ensure the DSL responds in line with the 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance. https://www.gov.uk/government/publications/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people
- store the device securely.

If an indecent image has been taken or shared on our network or devices, we will act to block access to all users and isolate the image. We will also:

- carry out a risk assessment which considers any vulnerability of pupils involved; including carrying out relevant checks with other agencies.
- inform parents/carers, if appropriate, about the incident and how it is being managed.
- make a referral to Children's Social Services and/or the Police, as deemed appropriate in line with the UKCCIS : 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
- provide the necessary safeguards and support for pupils, such as offering counselling or pastoral support.
- implement appropriate sanctions in accordance with our Behaviour Policy but taking care not to further traumatise victims where possible.
- consider the deletion of images in accordance with the UKCCIS: 'Sexting in schools and colleges: responding to incidents and safeguarding young people' guidance.
- delete images only when the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation.
- review the handling of any incidents to ensure that best practice was implemented.

12.5. Online Sexual Abuse and Exploitation (Including Criminal Exploitation):
The school will ensure that staff and pupils are aware of online child sexual abuse, including exploitation and grooming, the consequences, possible approaches which may be employed by offenders to target children and how to respond to concerns. The school will also disseminate this to parents where appropriate.

The school recognises online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL.

Trinity Christian School will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for pupils, staff and parents/carers.

We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.

We will ensure that the details for CEOP are visible and available to pupils and other members of our community via the School's website.

If the School is made aware of an incident involving online child sexual abuse and exploitation (including criminal exploitation), we will:

- act in accordance with our child protection policies and the Tameside Safeguarding Children Partnership Board's procedures.
- if appropriate, store any devices involved securely.
- make a referral to Children's Social Services (if required/appropriate) and immediately inform Greater Manchester police via 101, or 999 if a child is at immediate risk.
- carry out a risk assessment which considers any vulnerabilities of pupil(s) involved (including carrying out relevant checks with other agencies).
- inform parents / carers about the incident and how it is being managed.
- provide the necessary safeguards and support for pupils, such as, offering counselling or pastoral support.

- review the handling of any incidents to ensure that best practice is implemented.

We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using school provided or personal equipment.

Where possible, pupils will be involved in decision making and if appropriate, will be empowered to report concerns such as via the CEOP report website: https://www.ceop.police.uk/Safety-Centre/

If we are unclear whether a criminal offence has been committed, the DSL will obtain advice immediately from Tameside Safeguarding Children Partnership and/or Greater Manchester Police.

If anyone at Trinity Christian School is made aware of intelligence or information which may relate to child sexual exploitation (on or offline), it will be passed through to the Pheonix Team (Tameside's Child Sexual Exploitation Team) by the DSL cse.tameside@gmp.police.uk.
If pupils at other settings are believed to have been targeted, the DSL will seek support from Greater Manchester Police, and or the Phoenix Team, and or Tameside Safeguarding Children Partnership first to ensure that potential investigations are not compromised.

12.6. Indecent Images of Children (IIOC):
The school will ensure that all staff and pupils are made aware of the possible consequences of accessing Indecent Images of Children (IIOC). The school will also disseminate this to parents where appropriate.

We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.

We will seek to prevent accidental access to IIOC by using an internet Service provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.

If we are unclear whether a criminal offence has been committed, the DSL will obtain advice immediately from Tameside Safeguarding Partnership and/or Greater Manchester Police.

If anyone at Trinity Christian School is made aware of IIOC, we will:

- act in accordance with our Safeguarding and Child Protection policy and the relevant Tameside Safeguarding Children Partnership procedures.
- store any devices involved securely.
- immediately inform appropriate organisations, such as the Internet Watch Foundation (IWF), Greater Manchester Police or the LADO.

If anyone at Trinity Christian School is made aware that a member of staff or a pupil has been inadvertently exposed to indecent images of children, we will:

- ensure that the DSL is informed.
- ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk
- ensure that any copies that exist of the image, for example in emails, are deleted.

- report concerns, as appropriate to parents / carers.

If anyone at Trinity Christian School is made aware that indecent images of children have been found on the school provided devices, we will:

- ensure that the DSL is informed.
- ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk
- ensure that any copies that exist of the image, for example in emails, are deleted.
- inform the police via 101 (999 if there is an immediate risk of harm) and Children's Social Services (as appropriate).
- only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
- report concerns, as appropriate to parents / carers

If made aware that a member of staff is in possession of indecent images of children on school provided devices, we will:

- ensure that the DSL and the Headteacher are informed in line with our Safeguarding and Child Protection Policy for Managing Allegations Against Staff.
- inform the LADO and other relevant organisations in accordance with our Safeguarding and Child Protection Policy for Managing Allegations Against Staff.
- quarantine any devices until police advice has been sought

12.7. Cyberbullying:
Cyberbullying, along with all other forms of bullying, will not be tolerated at Trinity Christian School.

Full details of how we will respond to cyberbullying are set out in our Anti-Bullying, Behaviour Management, and Safeguarding and Child Protection policies.

12.8. Online Hate:
Online hate content, directed towards or posted by, specific members of the community will not be tolerated at Trinity Christian School and will be responded to the same way as cyberbullying.

The Police will be contacted if a criminal offence is suspected. If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL will obtain advice from Tameside Safeguarding Children Partnership and/or Greater Manchester Police.

12.9. Online Radicalisation and Extremism:
Trinity Christian School will take all reasonable precautions to ensure that pupils and staff are safe from terrorist and extremist material when accessing the internet on site.

Staff will annually complete the Government Prevent training:
https://www.gov.uk/guidance/prevent-duty-training

If anyone at Trinity Christian School is concerned that a child or parent / carer may be at risk of radicalisation online, the DSL will be informed immediately, and action will be taken in line with our Safeguarding and Child Protection Policy, and with advice from the Tameside Prevent Engagement Officer.

If we are concerned that member of staff may be at risk of radicalisation online, the DSL and the Headteacher will be informed immediately, and action will be taken in line with the Safeguarding and Child Protection Policy for Managing Allegations against Staff, along with advice from the Tameside Prevent Engagement Officer.

The practices and procedures in this Policy will be subjected to an annual review.