Trinity
Christian
School

wisdom
knowledge
truth

E-Safety including Social Media Policy

For you created my inmost being: you knit e together in my mother's womb. I praise you because I am fearfully and wonderfully made: your works are wonderful. I know that full well. My frame was not hidden from you when I was made in the secret place. When I was woven together in the depths of the earth, your eyes saw my unformed body. All the days ordained for me were written in your book before one of them came to be.

Psalm 139:13-16

The name of the lord is a strong tower; the righteous run to it and are safe.

Proverbs 18:10

Introduction

In today's society, children, young people and adults interact with technologies such as smart 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 can be greatly beneficial to all, but can also place children, young people and adults in danger. 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, including social media, 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.

Trinity Christian School aims to provide the right balance between controlling access to the internet and technology, setting rules and boundaries and educating students and staff about responsible use. Trinity Christian School is aware that pupils cannot be completely prevented from being exposed to risks both on and offline. Therefore, pupils should be empowered and educated so that they are equipped with the skills to make safe and responsible decisions as well as to feel able to report any concerns.

Online safety including social media

Pupils are not allowed access to their own devices during the working day. All members of staff need to be aware of the importance of good e-safety practice in the classroom in order to educate and protect the children in their care. Members of staff also need to be actively modelling. appropriate online behaviours compatible with their role and be informed about how to manage their own professional reputation online.

Expectations of students: see Acceptable Use Agreements KS1 and KS2

Trinity Christian School expects pupils to demonstrate self-respect:

- To represent themselves well by safeguarding their personal information online. To not publish others' personal information (including pictures, phone number, and full name) without their permission.
- To only access Internet resources that are appropriate in a school setting and to take responsibility for managing their time well.

Trinity Christian School expects pupils to respect others, their privacy, and property:

- To communicate respectfully, and to not use computers, phones, cameras or other technologies to bully, frighten or mistreat other people. To report to their parent or teacher any inappropriate material or hurtful communication they find, and to not pass it on.
- To not share passwords with others.
- To access only their own and other authorized files.
- To give credit for other peoples' work (including photos, words, and videos) that they use.
- To ensure that their actions do not distract or disturb those around them.
- To represent themselves and the school honourably including when online.
- To respect age restrictions for social media site use

Lead Person for E-Safety

The responsibility of managing e-safety is as follows: Our lead is the head teacher. The role of the E-Safety lead is to oversee and ensure that our e-safety policy is fully implemented. This includes ensuring that all staff receive e-safety information and child protection training as appropriate.

This policy will be made available to all adults, children, young people and parents/carers. This policy should also be read alongside the Safeguarding Policy and the Anti-Bullying Policy. Our E-Safety Code of Conduct. / Acceptable Use Agreements for staff, pupils and parents/carers.

We expect all adults in our organisation to follow our Acceptable Use Agreements for staff and parents/carers. All adults must:

- Use the internet and other forms of communication in a sensible, professional and polite way.
- Seek permission to use personal information or take photographs or images of other people.
- Report any concerns to the lead person for e-safety immediately.
- Be clear that confidentiality cannot be maintained if there is a concern about the welfare of a child or young person.
- Be vigilant in their use of devices in the light of the risk of scams that fraudsters may use to try to gain access to personal information

Good Practice for Staff

- Staff should not give their personal mobile phone number to pupils.
- Staff should not give their personal e-mail address to pupils.
- Pupils are not old enough to have a social networking site account but should any pupil violate this and approach staff to be 'friends' with them on a social networking site staff will refuse and refer to the E-Safety lead in school who will contact the parents.

What are the risks to pupils? There are many potential risks for children and young people including:

- Accessing age inappropriate or illegal websites.
- Receiving unwanted or upsetting text or e-mail messages or images.
- Being "groomed" by an adult with a view to meeting the child or young person for their own illegal purposes including sex, drugs or crime.
- Viewing or receiving socially unacceptable material such as inciting hatred or violence (potentially leading to radicalisation).
- Sending bullying messages or posting malicious details about others.

- Ignoring copyright law by downloading music and/or video or using homework cheat material.
- Building an inappropriate digital footprint

What else might be of concern? A child or young person who:

- Is becoming secretive about where they are going to or who they are meeting.
- Will not let you see what they are accessing on-line.
- Is using a webcam in a closed area, away from other people.
- Is accessing the web or using a mobile or Personal Data Assistant (PDA) for long periods and at all hours.
- Clears the computer history every time they use it.
- Receives unexpected money or gifts from people they don't know.

An adult who:

- Befriends a child/children on the internet or by text messaging.
- Has links to children on their Facebook or other social network site; especially if they work in a position of care.
- Is secretive about what they are doing and who they are meeting.

Supporting Parents

With the current speed of on-line change, some parents and carers have only a limited understanding of online risks and issues, including the risks particularly associated with social media. Parents may underestimate how often their children come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond. Some of the risks could be:

- Accessing material that is not age appropriate.
- Unwanted contact
- Being 'groomed' by an adult with a view to meeting the child or young person for their own illegal purposes including sex, drugs or crime.
- Viewing or receiving socially unacceptable or extremist material such as inciting hatred or violence, which may lead to radicalisation.
- Sending bullying messages or posting malicious details about others.
- Ignoring copyright law by downloading music, video or even homework cheat material.

The school will therefore seek to provide information and awareness to both pupils and their parents through:

- Giving information on safety features that are being applied at school and can be applied at home.
- Curriculum activities involving raising awareness around staying safe online.
- Information included in letters, newsletters and the school's website.
- Parents evenings / sessions.
- High profile events / campaigns e.g. Safer Internet Day Safer Internet Day 2021 | Safer Internet Centre

What do I do if I'm concerned? If you have any concerns, speak to the lead for e-safety immediately. They will take action as detailed in the Safeguarding Policy. You can also contact the Child Exploitation and Online Protection Centre (CEOP) for advice on 0870 000 3344 or via their website – www.ceop.gov.uk.

Contacts for referring

For contact details of organisations to which concerns are referred, please see the Safeguarding Policy. The following organisations may also be contacted with e-safety concerns:

- CEOP: This is a National Crime Agency body who will act on reports of any unknown person trying to make contact with a child via the internet. www.ceop.gov.uk.
- Internet Watch Foundation (IWF): Any instances of harmful content, including child sexual abuse images or incitement to racial hatred content should be reported to IWF – www.iwf.org.uk.Other

Useful Contacts

- NSPCC: Tel: 0808 800 5000
- Young people can get help and advice at:
- www.childline.org.uk or www.there4me.com. Tel: 0800 1111

For advice and resources about safe internet usage and concerns including bullying and hacking, visit: www.thinkuknow.co.uk

Minimising the Risks

Trinity Christian School will:

- Educate pupils about what they are accessing online and the associated risks.
- Maintain subscription to Norton Protection and review termly the blocks and filters that are in place.
- If pupils still discover unsuitable websites, they must be reported to the E-Safety Lead.
- Make additional checks to ensure that filtering is appropriate, effective and reasonable.
- Set up all school computers to default to Norton Protection.
- Keep the computers in a general space where staff can monitor what is going on.
- Explain the risks of giving out personal details online.
- Talk about how strangers can easily mislead and pretend to be someone else while online, e.g. by using misleading e-mails, photographs of other people, telling lies about their age, school, hobbies etc.
- Encourage children and young people to think carefully about what photographs or videos they use or post online. They can be used and tampered with by other people, or they may not be appropriate.
- Advise children and young people to only text, chat or use a web cam with people they know in real life.
- Talk about how to identify spam messages or junk mail and how to delete them. This also applies to messages from people they do not know, or opening attachments.
- Discuss how people hide their identities online and the importance of never meeting new online "friends" for real.
- Make sure children and young people understand they can always talk to us or their parents and/or carers about anything that makes them feel uncomfortable.
- Look on the internet together for information about how to deal with or report problems.

- Talk about how/when information or images get on to the internet, they can never be erased.
- Ban the use of mobile phones and/or other personal devices by pupils during school hours.

Cyber Bullying

Any reports of cyber bullying will be taken extremely seriously by Trinity Christian School and procedures will be followed as stated in the Anti-Bullying policy.

Links to other policies:

- Anti-bullying Policy
- Safeguarding Policy

Social Media Policy reviewed February 2015
E-Safety Policy Approved by governors: October 2015
E-Safety and Social Media Policies merged April 2018
Policy reviewed: September 2021

Next review: September 2023