TRINITY SCHOOL

Online Safety policy

A Procedural Guide

Date of Document: January 2023

Signed……. Chair/Vice Chair of Governors

Trinity School

Online Safety Policy

Everyone has the right to access to the internet and all the benefits it offers. It is important that we prepare our young people for a world increasingly dependent on the use of technology in the home and workplace. There is a separate social media policy which all staff should be aware of and adhere to.

We are aware of the potential harm from some material that's exists on the Internet. The school will ensure that students will remain safe online through the use of safe filtering and parents are informed of use of computers in school and sign the internet use agreement form. Social media and the internet can provide a wide range of content, some of which is harmful. We as a school will take the steps outlined in this policy to support our staff and students in staying safe on-line.

This policy also includes the social networking policy for staff and the staff acceptable use agreement.

Staying safe on-line

E –safety skills will be specifically taught through the computing and ICT lessons and opportunities for reinforcement identified across the curriculum including but not limited to PSHE and life skills. These lessons begin as part of any work using the internet.

- Students are encouraged to discuss their internet use and be open about their experiences.
- Students will be taught to use reputable search engines and be supported to critically evaluate the information they receive, at a level appropriate to their understanding.
- Students will be encouraged to report any content which makes them feel uncomfortable or unsafe.
- All screen time is to be overseen by a member of staff. Students should only use the internet, including on mobile devices where they can be monitored.
- Staff will receive training to support keeping our students safe on-line. This will include providing students with the skills to use the internet and social media safely outside school.
- Staff will be aware of and compliant to the school's e-safety, acceptable use and social media policies. New staff are provided with these during induction.

The e-safety policy relates to other policies including those for ICT and Computing, bullying and for child protection. It also incorporates the Acceptable use policy for staff and the social networking policy. (Appendix 1 and 2)

Managing the infrastructure

The school is responsible for ensuring that the school infrastructure is as safe and secure as is reasonably possible and that the polices and procedures within this policy are implemented.

- The school network has user-defined policies ensuring secure documents are only accessible by specific users.
- The school has educational, filtered secure broadband connectivity.
- Internet access is filtered for all users to keep users safe, including from sexual, terrorist and extremist content.
- Part of our duty of care is to ensure that staff, students and visitors report any unblocked/ unfiltered content including sexual, terrorist and extremist content that has possibly got through the filtering.
- A record of any unsuitable content that has been blocked will be obtained through LGfl and Elementary ICT support who manage the network.
- Devices may only be connected to the network (including the wireless network) with the express permission of the Head teacher, I.T Department.
- Staff access to the management information system is controlled through a separate password for data security purposes. Staff only have access to the modules they require for their role and passwords are not shared.

Personal devices

- Personal devices (such as mobile phones) brought into school are entirely at the owner's risk. The school accepts no responsibility for the loss, theft or damage of any phone or handheld device bought into school.
- Staff should not use their personal devices/phones when contacting pupils or parents: there should be access to a school phone.
- The taking, recording and sharing of images, video or audio on a personal device is forbidden. School devices are available for this purpose.

Radicalisation

- In accordance to the Prevent policy, all staff have the responsibility for identifying staff/ students who have become at risk of radicalisation.

Concerns can arise not only from use of school equipment but also content held on devices such as personal mobiles phones with internet access. Any content that causes concerns must be reported in line with the safeguarding policy.

Use of digital images

- Parents/ guardians should sign the digital media release form to give their consent before photographs are used.
- Digital media should be used in accordance with the home/school agreement.
- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks associated with publishing their own images on the internet e.g. on social networking sites.
- Pupil's full names should not be use anywhere on a website or blog, particularly in association with photographs.

Cyber - Bullying

- Cyber bullying is defined as bullying that takes place using electronic technology. Electronic technology includes devices and equipment such as cell phones, computers, and tablets as well as communication tools including social media sites, text messages, chat, and websites.

- Cyber bulling differs from regular bullying because it can take place out of school and at any time of the day or night.

- Cyberbullying messages and images can be posted anonymously and distributed quickly to a very wide audience. It can be difficult and sometimes impossible to trace the source.

- All members of the school community are to be aware of bullying as an issue and must follow the guidelines in the school Anti-bullying policy, regardless of where or when the bullying has taken place.

Reporting concerns

The designated lead for E-Safety at Trinity School is Sandra Lee (TLR/DPO).

Guidance for reporting concerns regarding a pupil.

- All concerns must be reported in line with the behaviour and safeguarding policies. Please see the flow chart bel

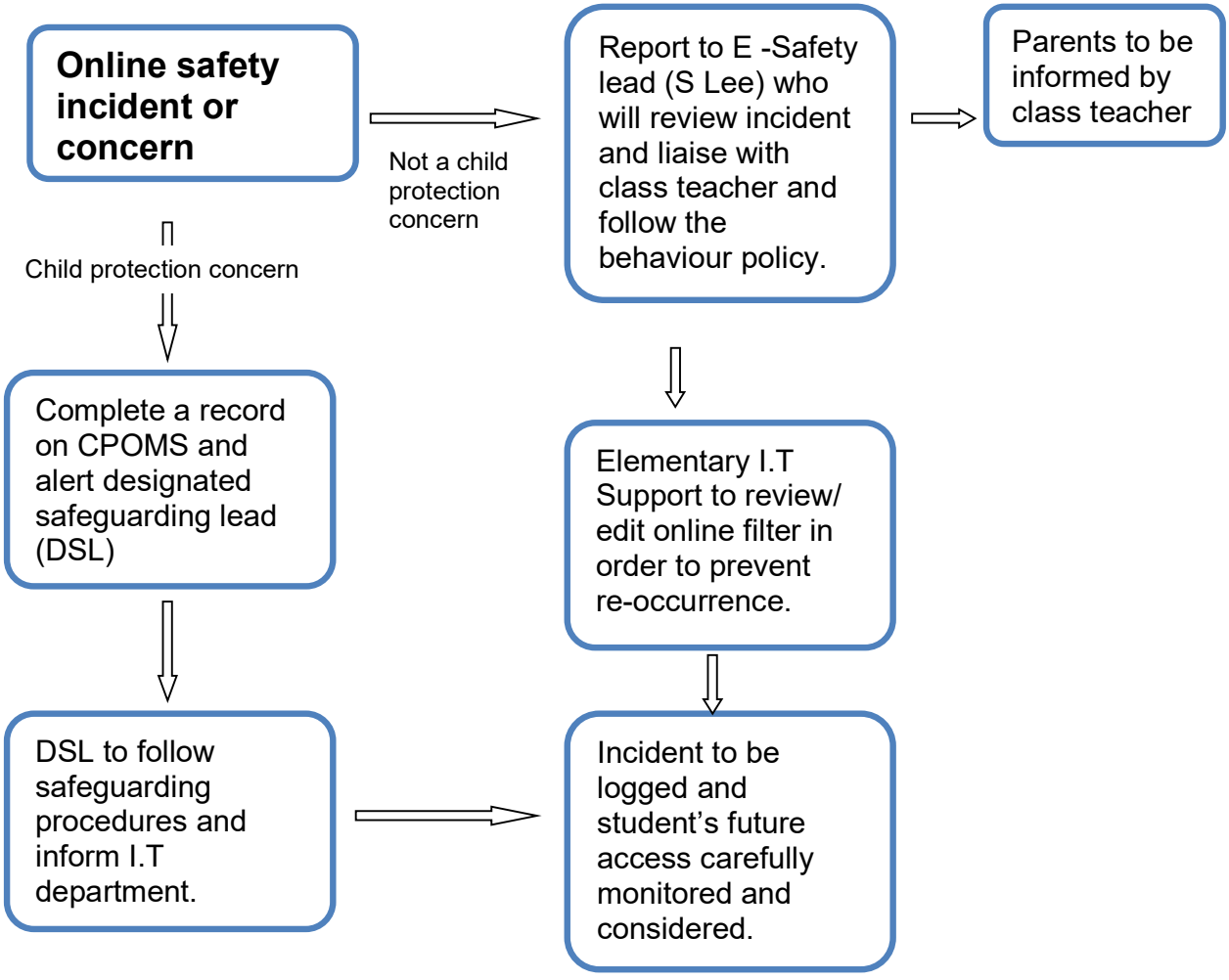
Guidance for reporting concerns regarding a member of staff or volunteer.

- All concerns regarding the behaviour or well-being of a member of staff or volunteer should be reported to the Head teacher.
- All concerns regarding the Head teacher should be reported to the chair of governors.

Guidance for reporting an incident outside of school

- Parents/carers who are reporting an online safety concern should report to the school in the first instance, who will follow procedures and attempt to resolve the incident. If this is not possible the incident may require referral to an outside agency.

Reporting an online safety concern for pupils



Trinity School Policy for the use of Social Networking.

Introduction to the Policy

This policy will apply to all paid employees of the school and extends to other workers engaged to work at Trinity School (including agency/supply, volunteers and external contracted agencies).

The school is aware and acknowledges that increasing numbers of adults and children are using social networking sites.

The widespread availability and use of social networking application bring opportunities to understand, engage and communicate with audiences in new ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our reputation.

This policy and associated guidance is to protect staff/other workers and advise school leadership on how to deal with potential inappropriate use of social networking sites.

For example, our use of social networking applications has implications for our duty to safeguard children, young people and vulnerable adults.

The policy requirements in this document aim to provide this balance to support innovation whilst providing a framework of good practice.

Purpose
The purpose of this policy is to ensure:

- That the school is not exposed to legal risks
- That the reputation of the school is not adversely affected
- That our users are able to clearly distinguish where information provided via social networking applications is legitimately representative of the school.

Facebook is targeted at older teenagers and adults. They have a no under-13 registration policy and recommend parental guidance for 13 to 16 year olds.

The following are extracts from Facebook privacy policy:
"*If you are under age 13, please do not attempt to register for Facebook or provide any personal information about yourself to us. If we learn that we have collected personal information from a child under age 13, we will delete that information as quickly as possible. If you believe that we might have any information from a child under age 13, please contact us*".

"*We strongly recommend that minors 13 years of age or older ask their parents for permission before sending any information about themselves to anyone over the Internet and we encourage parents to teach their children about safe internet use practices.*

This guidance is to advise and protect staff and other workers from accusations of improper relationships with pupils

Scope
This policy covers the use of social networking applications by all school stakeholders, including, employees, Governors, other workers and pupils. These groups are referred to collectively as 'school representatives' for brevity.

The requirements of this policy apply to all uses of social networking applications which are used for any school related purpose and regardless of whether the School representatives are contributing in an official capacity to social networking applications provided by external organisations.
Social networking applications include, but are not limited to:

1. Collaborative spaces, such as Facebook
2. Online discussion forums, such as netmums.com
3. Blogs, for example Blogger
4. Media sharing services, for example YouTube
5. 'Micro-blogging' applications, for example Twitter
6. Messaging services such as Whattsapp.

All school representatives should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with the School's Equality and Diversity Policy.

Use of Social networking sites in work time
Use of social networking applications in work time for personal use only is **not permitted,** unless permission has been given by the Head teacher.

Social Networking as part of School Service

- All proposals for using social networking applications as part of a school service (whether they are hosted by the school or by a third party) must be approved by the Head teacher first

- Use of social networking applications which are not related to any school services (for example, contributing to a wiki provided by a professional association) does not need to be approved by the Head teacher. However, school representatives must still operate in line with the requirements set out within the policy
- School representatives must adhere to the following Terms of Use. The Terms of Use below which apply to all uses of social networking applications by all school representatives. This includes, but is not limited to, public facing applications such as open discussion forums and internally-facing uses such as project blogs regardless of whether they are hosted on school network or not.
- Where applications allow the posting of messages online, users must be mindful that the right to freedom of expression attaches only to lawful conduct. Trinity School expects that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of Use.

Terms of Use

Social Networking applications

- Must not be used to publish any content which may result in actions for defamation, discrimination, breaches of copyright, data protection or other claim for damages. This includes but is not limited to material of an illegal, sexual or offensive nature that may bring the school into disrepute.
- Must not be used for the promotion of personal financial interests, commercial ventures or personal campaigns
- Must not be used in an abusive or hateful manner
- Must not be used for actions that would put school representatives in breach of school codes of conduct or policies relating to staff.
- Must not breach the school's misconduct, equal opportunities or bullying and harassment policies
- Must not be used to discuss or advise any matters relating to school matters, staff, pupils or parents
- No staff member should have a pupil or former pupil under the age of 18 as a 'friend' to share information with
- Employees should not identify themselves as a representative of the school
- References should not be made to any staff member, pupil, parent or school activity / event unless prior permission has been obtained and agreed with the Head Teacher
- Staff should be aware that if their out-of-work activity causes potential embarrassment for the employer or detrimentally effects the employer's reputation then the employer is entitled to take disciplinary action.

Violation of this policy will be considered as gross misconduct and can result in disciplinary action being taken against the employee up to and including termination of employment.

- **Guidance/protection for staff on using social networking**
- No member of staff should interact with any pupil in the school on social networking sites
- No member of staff should interact with any ex-pupil in the school on social networking sites who is under the age of 18
- This means that no member of the school staff should request access to a pupil's area on the social networking site. Neither should they permit the pupil access to the staff members' area e.g. by accepting them as a friend.
- Where family and friends have pupils in school and there are legitimate family links, please inform the head teacher in writing. However, it would not be appropriate to network during the working day on school equipment.
- It is also advised that no member of staff should interact with any parent of a child in the school on social networking sites.
- It is illegal for an adult to network, giving their age and status as a child
- Information regarding pupils will never be made by a member of staff
- Staff will not share information or make comment on the performance of colleagues using social networks.
- If you have any evidence of pupils or adults using social networking sites in the working day then you should contact the Headteacher

- **Guidance/protection for Pupils on using social networking**
- No pupil under 13 should be accessing social networking sites. This is the guidance from both Facebook and MSN. There is a mechanism on Facebook where pupils can be reported via the Help screen; at the time of time of writing this policy the direct link for this is:
http://www.facebook.com/help/contact.php?show_form=underage
- No pupil may access social networking sites during the school working day
- No pupil should attempt to join a staff member's areas on networking sites. If pupils attempt to do this, the member of staff is to inform the Head teacher. Parents will be informed if this happens
- No school computers are to be used to access social networking sites at any time of day.
- Any attempts to breach firewalls will result in a ban from using school ICT equipment other than with close supervision
- Please report any improper contact or cyber bullying to you tutor / class teacher in confidence as soon as it happens.
- We have a zero tolerance to cyber bullying

Child protection guidance

- If the Headteacher receives a disclosure that an adult employed by the school is using a social networking site to contact a pupil or share information about a pupil then a safeguarding referral will be made.

Cyber Bullying

- By adopting the recommended no use of social networking sites on school premises, Trinity School protects themselves from accusations of complicity in any cyber bullying through the provision of access.
- Parents should be clearly aware of the school's policy of access to social; networking sites.
- Where a disclosure of bullying is made, schools now have the duty to investigate and protect, even where the bullying originates outside the school.
- Once disclosure is made, investigation will have to involve the families. This should be dealt with under the school's adopted anti bullying policy.
- If parent / carers refuse to engage and bullying continues, it can be referred to the police as harassment
- This guidance can also apply to text and mobile phone cyber bullying.

Appendix 1.

Trinity School

ICT Acceptable Use: Agreement form

EMAIL / INTERNET / INTRANET / NETWORK USAGE POLICY

- I will only use the school's Email / Internet / Intranet for Professional purposes or for uses deemed 'reasonable' by the Head and Governing Body.
- I will only use the approved, secure school email system for school business.
- I will not browse, download or send material that could be considered offensive to colleagues.
- I will report any accidental access to inappropriate materials to the appropriate line manager.
- I will not download or install any software or resources from the Internet that can compromise the safety of the network, or is not adequately licensed.
- I will ensure all documents are saved, accessed and deleted in accordance with the school's network security and confidentiality protocols.
- I will not connect a computer, laptop, or any personal device to any computer / network / Internet without the permission of the network manager.
- I will not use personal digital cameras or mobile phones for transferring images of pupils or colleagues.
- I will not store any images of staff or pupils other than on school equipment.
- I will not use photographs of the school and/or pupils for personal use whatsoever.
- I will ensure I am aware of digital safety-guarding issues so they are appropriately embedded in my classroom practice.
- I will not allow unauthorised individuals to access my Email / Internet / Intranet.
- I will never leave a computer system logged on and unattended at any time

- I understand that all Internet usage will be logged and this information could be made available to my manager on request.
- I agree and accept that any computer or laptop loaned to me by the school, is provided solely to support my professional responsibilities and that I will notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- I will report any content which raises concern in line with the appropriate policy
- I understand that failure to comply with the Usage Policy could lead to disciplinary action.
- I understand that my details may be shared with external sources for IT purposes

User Signature

I agree to abide by the above Acceptable Usage Policy.

Signature …….…… Date ……

Full Name …….....(printed)

Job title . . . . . .

Authorised Signature (Head Teacher)

Is this member of staff temporary? NO / YES If yes, contract end date: ……

I approve this email account / connection to the Internet / Intranet.

Signature ……..... Date ……

Full Name ……....…(printed)

We recommend: One copy is retained by member of staff | Second copy for school file