TRINITY SCHOOL

Online Safety Policy

Date of Document: 08.11.23
First Revision:
Second Revision:
Third Revision:
Fourth Revision:

Signed: _____ (Chair of Governors)

Author:

Purpose

This Online Safety Policy outlines the commitment of Trinity School to safeguard members of our school community online in accordance with statutory guidance and best practice.

This Online Safety Policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Trinity School will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

The purpose of this policy is to ensure that all children and young people at our school are able to use the internet and other online resources in a safe and responsible manner. This policy outlines the expectations for online behaviour, as well as the consequences of inappropriate use.

We aim to:

- Protect our vulnerable students: We recognise that some of our students may be more vulnerable to harm from online activities, and we are committed to taking all necessary measures to protect them.
- Promote responsible use: We encourage our students to use the internet for educational purposes and to avoid any behaviour that could be considered inappropriate or illegal. We want to ensure that our students are able to use the internet in a way that is both safe and productive.
- Raise awareness: We recognise that online safety is an ongoing concern, and we are committed to raising awareness about the potential risks and challenges of using the internet. We provide training and educational resources to our students, staff, and parents to ensure that everyone in our school community understands the importance of online safety.
- Encourage parental involvement: We believe that parents play a vital role in promoting online safety, and we encourage all parents to become involved in monitoring their child's online activity and reporting any concerns or incidents to the school. We want to work together with parents to create a safe and supportive online environment for all of our students.
- Inform staff how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.

Overall, the purpose of this policy is to promote a culture of responsible and safe internet use in our school. We believe that by working together, we can create a safe and supportive online environment for all of our students.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk as stated within Keeping Children Safe in Education (2023):
Content: being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
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.
Conduct: personal 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; and
Commerce - risks such as online gambling, inappropriate advertising, phishing and or financial scams.
(DfE Keeping Children Safe in Education 2023)
• To inform staff how to manage their own professional reputation online and demonstrate appropriate online behaviours compatible with their role.
• To provide opportunities for parents/carers to develop their knowledge of e-safety.
• To ensure awareness amongst all members of Trinity school that 'online actions can have offline consequences'

Legislation and guidance
This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice to schools.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

Roles and Responsibilities

Governors

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure that all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school. That any serious concerns are reported to the Governors.

The Designated Safeguarding Lead

The Assistant Head for Safeguarding takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents

- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety. Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

Network Manager/ Technical Staff

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the school's ICT systems on a minimum monthly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

Teaching and Support Staff

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy and an up to date awareness of e-safety matters.
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use where applicable.
- Knowing that the Assistant Head for Safeguarding is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes by reporting to The Assistant Head for Safeguarding or the IT Manager.
- Following the correct procedures by consulting the IT Manager to complete the action, if they need to bypass the filtering and monitoring systems for educational purposes.

- Working with the Assistant Head for Safeguarding to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'.
- Abide by the Data Protection Policy and report any breaches to the Data Protection Officer.
- Digital communications with pupils and parents / carers (email / voice) should be on a professional level.
- Students/ pupils understand and follow Online Safety rules to the best of their ability.
- In lessons where internet use is planned students / pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- They model safe, responsible, and professional online behaviours in their own use of technology, including out of school and in their use of social media

Parents and Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about national / local e-safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good e-safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events
- equipment and resources provided by the school
- their children's personal devices in the school (where this is allowed).

Acceptable Use Policy

The ICT Acceptable Use Policies for Staff and Students form a core part of this E-Safety policy. (The staff policy includes responsibilities staff have for visitors, and responsibilities visitors have.) Breaches of an acceptable use policy can lead to civil, disciplinary and criminal action been taken against staff, pupils and members of the wider school community. All trainee teachers and staff will be expected to read our ICT Acceptable Use Policies and sign the appropriate consent documentation. Appendix 1

All parents/ carers will be asked to read an ICT acceptable use policy for their child. Parents / carers should discuss the ICT acceptable use policy for pupils with their child, where appropriate. Appendix 2

Remote Working

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Installing anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way that would violate the school's terms of acceptable use. Work devices must be used solely for work activities.
If staff have any concerns over the security of their device, they must seek advice from the ICT Manager.

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.

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 on social network sites

- 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.

Further staff guidance for personal use and social networking will be discussed as a part of the staff induction process, annual safeguarding training.

Mobile Device Use

Staff (both permanent and agency) -

- Staff must not use mobile phones during school hours (with the exception of break times and agreed emergencies). This includes calling, texting and checking phones for any reason. Phones must not be used during lessons for filming, recording or use of apps e.g. YouTube, calculator, weather.
- Staff must not have phones on their person at any time (expect when on break or for agreed emergencies). Phones should be kept in bags in locked cupboards, locked filing cabinets or staffroom lockers.
- Staff must not connect phones to ICT equipment for charging.

- When phones are used during breaks, they must be used in designated staff rooms only and not in corridors, classrooms or other areas of the school where pupils may be.
- In emergency situations staff may request to have their phones on them. This must be agreed by a phase manager and may only be granted for exceptional situations e.g. relative with emergency health issues, emergency test results. Any other messages for staff must be given to the school office, who will then pass this on.
- The exception to this will be:
    - Deputy Head Teachers and Head Teacher – who may need to be contacted for emergency response procedures.
    - Managers who may need to use mobiles to contact the office and other managers if there is an emergency situation or the phone system stops working.
    - The site team – who will need to contact each other throughout the day regarding various aspects of their roles (urgent health and safety issues, fire alarms).
    - The after-school clubs' manager – he will use his phone to make and receive calls to parents
    - Staff taking pupils for offsite visits e.g. community sport, college links.
- This policy will go out to staff at the beginning of each year. It will also be included in the induction manual.
- The safeguarding leaflet given to agency staff will contain the key details of this policy.

Parents, Visitors and Professionals –

- Parents/visitors are not permitted to use phones when on the school premises.
- If this occurs, staff must ensure parents delete any recorded content on their phones before they leave. If parents refuse or they have concerns that recordings may involve safeguarding issues, staff should report this to a Designated Safeguarding Lead and the Data Protection Officer as soon as possible.
- Parents/visitors will be reminded that mobile phone use is not allowed by the staff escorting and working with them for coffee mornings, parents training, school tours, etc.
- Parents/visitors may be permitted to photograph resources during training sessions provided no pupils are present and they do not take photos of photographs (e.g. schedules with photos)
- Parents/visitors may use phones during review meetings conducted in the conference room at the front of school, during medicals conducted in the medical room or in managers offices, for the purposes of sharing relevant photos, videos and information with other professionals.
- Parents may use phones to take photos and videos during Christmas concerts and prizegiving. They will be reminded by the staff involved that any photos or videos must not be published to social media or shared in any other way.
- Contractors who are onsite during school hours must not use phones in corridors and spaces where pupils are present. This will be communicated to them via the premise's manager.
- The safeguarding leaflet given to visitors will contain the key details of this policy

Pupils –

- Pupils are not permitted to bring mobile phones to school as a general rule.
- Students in the FEC who are independent travelers may bring a phone to school where this is agreed with the Head of the FEC. Phones will then be handed to the Head of School to be kept securely until the end of the day.
- Parents will be reminded of this policy via an annual letter home.

- Phones brought into school by pupils may be removed and kept safe by the class teacher or teaching assistants if they are concerned about their inappropriate use. Parents will also be informed and reminded of the school policy.
- While we will always take reasonable measures to keep all pupils' property safe, Trinity cannot accept any liability for pupils' phones when brought into school. We recommend that independent travelers only use valuable phones when outside school.

Monitoring/How do we know this approach is working?

- Minimal incidents of staff using phones are reported. Any incidents are dealt with swiftly and appropriately. All staff are aware of the policy and adhere to it. Incidents are monitored in phase. Any significant or repeated incidents are shard with SLT, who will consider further action. Persistent failure to adhere to this policy without exceptional circumstances could be considered and investigated as misconduct under the School's Disciplinary Procedure.
- Minimal incidents of parents and visitors using phones on site. All incidents are dealt with swiftly and appropriately. Incidents are monitored in phases and by the training team. Any significant or repeated incidents are shard with SLT, who will consider further action.
- Parents and visitors are consistently informed about the above at key events via reminders from staff and posters on display.

Cyber-bullying

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy and anti-bullying policy.)

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, where appropriate, Trinity will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

All staff and governors receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training.

The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

The Assistant Head for Safeguarding will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

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.

Education – Pupils

Staying safe on-line

Online safety skills will be discreetly taught through the computing and ICT lessons and opportunities for reinforcement identified across the curriculum including but not limited to PSHE/ RSE and life skills in KS 3/4. Online safety is also embedded in use of IT equipment in KS1/2/5. 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 online safety, acceptable use and social media policies. New staff are provided with these during induction in this policy.
- Online Safety rules to be placed near IT equipment with internet connection.
- Staff may deliver specific online safety lessons relating to current issues.

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 pupils, cyber bullying policy, mobile phone use policy and the social networking policy.

Education of Parents

Many parents and carers have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children's online experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, emails, parent platforms
- Parents evenings
- Family support team
- Reference to external websites
- Publishing the online safety policy on the school website.

Technical – Infrastructure

The school is responsible for ensuring that the school infrastructure is as safe and secure as is reasonably possible and that the policies 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 tools provided by the school's internet service provider LGfl.
- 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.

Filtering

Filtering systems are only ever a tool in helping to safeguard children when online and schools have an obligation to "consider how children may be taught about safeguarding, including online, through teaching and learning opportunities, as part of providing a broad and balanced curriculum" (KCSIE 2023)

Schools in England (and Wales) are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering" (Prevent Duty)

- The school manages access to content across its systems for all users. The filtering provided meets the standards defined in the UK Safer Internet Centre Appropriate filtering. This is done through LGFL Webscreen filtering provided by LGFL.
- Filtering provision will be checked annually by the Assistant Head of Safeguarding and IT Manager.
- Access to online content and services is managed for all users
- There are established and effective routes for users to report inappropriate content
- There is a clear process in place to deal with requests for filtering changes – application must be made to IT manager
- Filtering logs are regularly reviewed to check for breaches of the filtering policy, which are then acted upon.
- Access to content through non-browser services (e.g. apps and other mobile technologies) is managed in ways that are consistent with school policy and practice.

Monitoring

The school follows the UK Safer Internet Centre Appropriate Monitoring guidance and protects users and school systems through the use of the appropriate blend of strategies. These include:

- physical monitoring (adult supervision in the classroom)
- filtering logs are regularly analysed and breaches are reported to senior leaders
- pro-active alerts inform the school of breaches to the filtering policy, allowing effective intervention.
- where appropriate, school technical staff monitor and record the activity of users on the school technical systems.

Technical Security

The school technical systems will be managed in ways that ensure that the school meets recommended technical requirements:

- there will be regular reviews and audits of the safety and security of school technical systems
- servers, wireless systems and cabling are securely located and physical access restricted
- there are rigorous and verified back-up routines, including the keeping of network separated (air-gapped) copies off-site or in the cloud
- all users have clearly defined access rights to school technical systems and devices.
- Details of the access rights available to groups of users will be recorded by the Network Manager (or other person) and will be reviewed, at least annually.
- all users (adults and learners) have responsibility for the security of their username and password and must not allow other users to access the systems using their log on details. Users must immediately report any suspicion or evidence that there has been a breach of security
- all school networks and system will be protected by secure passwords. Passwords must not be shared with anyone. All users will be provided with a username and password by the Network Manager who will keep an up-to-date record of users and their usernames
- the master account passwords for the school systems are kept in a secure place, e.g. school safe. It is recommended that these are secured using two factor authentication for such accounts.
- records of learner usernames and passwords for learners can be kept in an electronic or paper-based form, but they must be securely kept when not required by the user. Password complexity for learners may be reduced and should not include special characters.
- The Network Manager is responsible for ensuring that all software purchased by and used by the school is adequately licensed and that the latest software updates (patches) are applied.
- an appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed)
- appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems and devices from accidental or malicious attempts which might threaten the security of the school systems and data. The school infrastructure and individual workstations are protected by up-to-date endpoint (anti-virus) software.

- an agreed policy is in place (to be described) regarding the extent of personal use that users (staff / learners / community users) and their family members are allowed on school devices that may be used out of school
- an agreed policy is in place (to be described) that allows staff to/forbids staff from downloading executable files and installing programmes on school devices
- an agreed policy is in place regarding the use of removable media (e.g., memory sticks) by users on school devices.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured in accordance with the school Personal Data Policy

Reporting concerns

All concerns should be reported to the Assistant Head of Safeguarding.

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 below.

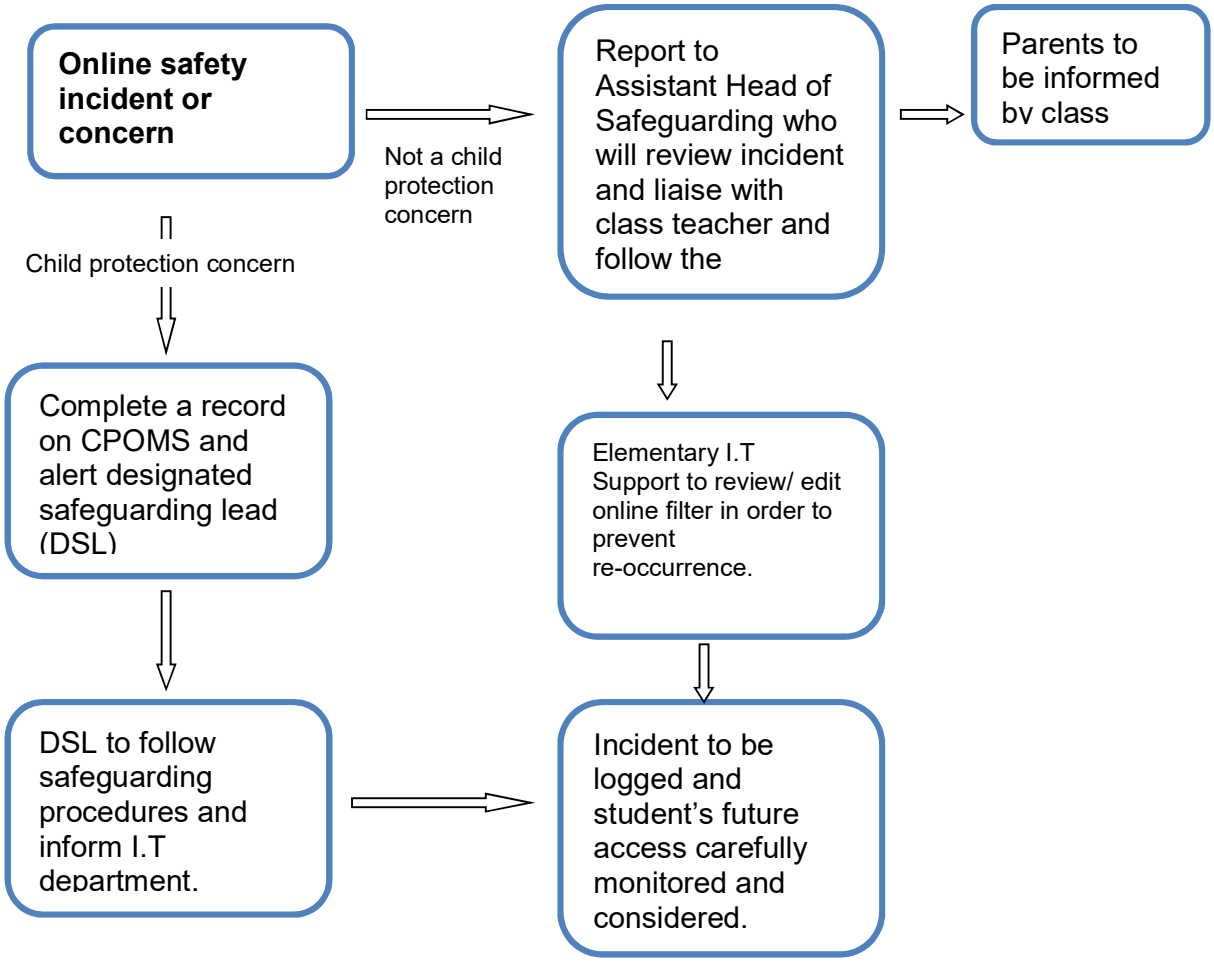
Guidance for reporting concerns regarding a member of staff or volunteer.

- 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'S ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of pupil:	

When I use the school's ICT systems (like computers) and get onto the internet in school I will:
• Ask a teacher or adult if I can do so before using them
• Only use websites that a teacher or adult has told me or allowed me to use
• Tell my teacher immediately if:
  ○ I select a website by mistake
  ○ I receive messages from people I don't know
  ○ I find anything that may upset or harm me or my friends
• Use school computers for school work only
• Be kind to others and not upset or be rude to them
• Look after the school ICT equipment and tell a teacher straight away if something is broken or not working properly
• Only use the username and password I have been given
• Try my hardest to remember my username and password
• Never share my password with anyone, including my friends
• Never give my personal information (my name, address or telephone numbers) to anyone without the permission of my teacher or parent/carer
• Save my work on the school network
• Check with my teacher before I print anything
• Log off or shut down a computer when I have finished using it
I agree that the school will monitor the websites I visit and that there will be consequences if I don't follow the rules.	

Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

TRINITY SCHOOL'S ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS

Name of staff member/governor/volunteer/visitor:

When using the school's ICT systems and accessing the internet in school, or outside school on a work device (if applicable), I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Take photographs of pupils without checking with teachers first
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I will only use the school's ICT systems and access the internet in school, or outside school on a work device, for educational purposes or for the purpose of fulfilling the duties of my role.

I agree that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the Assistant Head of Safeguarding and ICT manager know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (staff member/governor/volunteer/visitor):	**Date:**