Online Safety Policy

This policy has been adopted by all schools within The Golden Thread Alliance

Approved by:	Board of Trustees	**Date:** September 2024
Last reviewed on:	September 2024	
Next review due by:	April 2025	

Contents

1. Aims

Our trust and schools aim to:

- Have robust processes in place to ensure the online safety of pupils, colleagues, volunteers and Governors
- Identify and support groups of pupils that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as 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, such as 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

2. 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 for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships and sex education
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

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.

The policy also takes into account the National Curriculum computing programmes of study.

Please note that any reference to Headteacher also applies to an *Acting* Headteacher.

3. Roles and responsibilities

3.1 The Board of Trustees

The Board of Trustees are responsible for;

- Evaluating and approving this policy at each review, ensuring that it complies with guidance and legislation
- Include Online Safety as part of the whole-trust approach to safeguarding
- The Trustee with responsibility for safeguarding will review the DfE filtering and monitoring standards, and action, in collaboration with the Trust Safeguarding Lead and Trust Online Safety Lead, what needs to be done to support the schools in meeting the standards, which include:
    - Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
    - Reviewing filtering and monitoring provisions at least annually;
    - Identify requirements for training

3.1 The Local Governing Committee

The Local Governing Committee has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The Local Governing Committee are responsible for;

- Monitoring Online Safety logs as provided by the Designated Safeguarding Lead (DSL) during monitoring visits
- Ensuring that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures

3.2 The Headteacher

The Headteacher (including *Acting* Headteacher) is responsible for;

- Ensuring that colleagues understand this policy, and that it is being implemented consistently throughout the school.
- Ensuring the school has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness.
- Ensuring that all colleagues undergo online safety training as part of child protection and safeguarding training, and ensure colleagues understand their expectations, roles and responsibilities around filtering and monitoring.
- Ensure that all colleagues 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.
- Ensure children are taught how to keep themselves and others safe, including keeping safe online.
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

3.3 The Designated Safeguarding Lead (DSL)

Details of the school's designated safeguarding lead (DSL) and deputy/deputies are set out in our child protection and safeguarding policy, as well as relevant job descriptions.

The DSL 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 Committee 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 IT Support Providers to make sure the appropriate systems and processes are in place
- Working with the Headteacher, IT Support Providers and other colleagues, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the Trust'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
- Evaluating and updating colleagues with relevant training on online safety (appendix 1 contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the Headteacher, Trust Safeguarding Lead, Trust Online Safety Lead and/or Governing Committee
- Undertaking annual Online Safety Audit in collaboration with the school computing lead and the Trust Online Safety Lead, that considers and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all colleagues, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The Trust Safeguarding Lead and Trust Online Safety Lead

The Trust Safeguarding Lead and Trust Online Safety Lead are 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
- Conducting regular checks of the Trust filtering and monitoring systems across all schools to ensure that they are fit for purpose
- Working with the ICT support providers to ensure this policy is implemented
- Provide advice and training to school DSLs in systems and processes with regard to this policy
- Providing regular safeguarding and child protection updates, including online safety, to all colleagues, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively
- Regular reporting to the Safeguarding Working Group

This list is not intended to be exhaustive.

3.5 The ICT Support Providers

The ICT Support Provider 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 regular checks and monitoring the school's ICT systems
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

This list is not intended to be exhaustive.

3.6 All Colleagues and Volunteers

All colleagues, including third parties and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (ICT and Acceptable Use Policy), and ensuring that pupils follow the school's terms on acceptable use
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by contacting the school's DSL, or Deputy DSL, immediately.
- Following the correct procedures by consulting the DSL, if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL 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'

This list is not intended to be exhaustive.

3.7 Parents and Carers

Parents and carers are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the Trust's ICT systems and internet (ICT and Acceptable Use Policy)

Parents and carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet
- Parent resource sheet – Childnet

3.8 Visitors and Members of the Community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (ICT and Acceptable Use Policy).

4. Educating Pupils about Online Safety

Pupils will be taught about online safety as part of the curriculum:

All schools have to teach:

- Relationships education and health education in primary schools

In **Key Stage (KS) 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

Pupils in **Key Stage (KS) 2** will be taught to:

- Use technology safely, respectfully and responsibly
- Recognise acceptable and unacceptable behaviour
- Identify a range of ways to report concerns about content and contact

By the **end of primary school**, pupils will know:

- That people sometimes behave differently online, including by pretending to be someone they are not
- That the same principles apply to online relationships as to face-to-face relationships, including the importance of respect for others online, including when we are anonymous
- The rules and principles for keeping safe online, how to recognise risks, harmful content and contact, and how to report them
- How to critically consider their online friendships and sources of information including awareness of the risks associated with people they have never met
- How information and data is shared and used online
- What sorts of boundaries are appropriate in friendships with peers and others (including in a digital context)
- How to respond safely and appropriately to adults they may encounter (in all contexts, including online) whom they do not know

The safe use of social media and the internet will also be covered in other subjects where relevant. Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some pupils with SEND.

5. Educating Parents and Carers about Online Safety

The school will raise parents and carers' awareness of internet safety in letters or other communications home, and in information via our website or parent/carer communication platforms. This policy will also be accessible to parents and carers.

If parents and carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher, the DSL or class teacher.

Concerns or queries about this policy can be raised with the Headteacher or The Trust Safeguarding Lead.

6. Cyber-Bullying

6.1 Definition

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.)

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we 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.

The school will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Class teachers will discuss cyber-bullying with their pupils.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All colleagues, Governors and volunteers (where appropriate) 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 and carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL 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.

6.3 Examining Electronic Devices

The Headteacher, and any member of staff authorised to do so by the Headteacher, can carry out a search and confiscate any school, Trust or pupil electronic device, including mobile phones, that they have reasonable grounds for suspecting:

- Poses a risk to colleagues or pupils, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is and consider the risk to other pupils and colleagues. If the search is not urgent, they will seek advice from the Headteacher or DSL
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the colleagues should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to Headteacher or DSL to decide on a suitable response. If there are images, data or files on the device that colleagues reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, colleagues will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent or carer refuses to delete the material themselves

If a colleague **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL or Headteacher immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our behaviour policy

Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial Intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Colleagues, pupils, parents and carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

The Golden Thread Alliance recognises that AI has many uses to help pupils learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness.

The Golden Thread Alliance will treat any use of AI by pupils to bully other pupils in line with our anti-bullying/behaviour policy.

Colleagues should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment (see appendix 2) where new AI tools are being used by the school/Trust.

7. Acceptable Use of the Internet in School

All pupils, parents, carers, colleagues, volunteers, Governing Committee and Governors are expected to sign an agreement regarding the acceptable use of the Trust's ICT systems and the internet (ICT and Acceptable Use Policy). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant.

Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by pupils, colleagues, volunteers, Governing Committee, Governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering system.

More information is set out in the acceptable use agreements in the ICT and Acceptable Use Policy.

8. Pupils using Mobile Devices in School (including Mobile Phones)

Pupils may bring mobile devices to school, but are not permitted to use them during school hours. Any devices brought to school must be handed in on arrival and will be stored securely by school staff during the school day.

Any breach of the behaviour policy or acceptable use agreement by a pupil may trigger disciplinary action in line with the school behaviour policy, which may result in the confiscation of their device, or other sanctions such as suspension or permanent exclusion.

9. Staff using Work Devices Outside School

All colleagies 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)
- Ensuring any external hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- Making sure the device locks if left inactive for a period of time
- Not sharing a school device among family or friends
- Installing anti-virus and anti-spyware software on non-school devices
- Keeping operating systems up to date by always installing the latest updates

Colleagues must not use the device in any way that would violate the school's terms of acceptable use, as set out in the ICT and Acceptable Policy.

Colleagues are permitted to occasionally use school ICT facilities for personal use subject to certain conditions as set out in the ICT and Acceptable Use Policy.

If colleagues have any concerns over the security of their device, they must seek advice from the ICT Support Service.

10. How the School Will Respond to Issues of Misuse

Where a pupil misuses the Trust's ICT systems or internet, we will follow the procedures set out in our policies on behaviour and ICT and internet acceptable use. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a colleague misuses the school's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff discipline and conduct policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police. They will also consider if the incident meets threshold for a LADO (Local Authority Designated Officer) referral or low-level concern, in line with the Managing Allegations Policy.

11. Training

All new colleagues will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation.

All colleagues will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all colleagues will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, threatening, harassing and misogynistic messages
    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help colleagues:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure pupils can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence pupils to make the healthiest long-term choices and keep them safe from harm in the short term

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, within their DSL training refresher, at least every two years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Child Protection and Safeguarding Policy.

12. Monitoring Arrangements

The DSL and Deputy DSLs log behaviour and safeguarding issues related to online safety.

This policy will be reviewed every year by the Trust Safeguarding Lead and Trust Online Safety Lead. At every review, the policy will be approved by the Board of Trustees. The review will be supported by the annual Online Safety Audit that considers and reflects the risks pupils face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

13. Links with Other Policies

This online safety policy is linked to our:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Staff Disciplinary and Conduct Policy
- Data Protection Policy and Privacy Notices
- Complaints Policy
- ICT and Acceptable Use Policy
- RSE Policy and Curriculum Guidance

Appendix 1: Online Safety Training Needs – Self-Audit for Colleagues

Adapt this form to suit your needs.

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of colleague/volunteer:	**Date**:
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in school?	
Are you aware of the ways pupils can abuse their peers online?	
Do you know what you must do if a pupil approaches you with a concern or issue?	
Are you familiar with the school's acceptable use agreement for staff, volunteers, governors and visitors?	
Are you familiar with the school's acceptable use agreement for pupils and parents/carers?	
Are you familiar with the filtering and monitoring systems on the school's devices and networks?	
Do you understand your role and responsibilities in relation to filtering and monitoring?	
Do you regularly change your password for accessing the school's ICT systems?	
Are you familiar with the school's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like training/further training?	

Appendix 2: Risk Assessment Template

HAZARD	WHO MIGHT BE HARMED AND HOW?	WHAT ARE YOU DOING ALREADY?	DO YOU NEED TO DO ANYTHING ELSE TO CONTROL THIS RISK?	ACTION: WHO?	ACTION: WHEN?	DONE