Thurgoland CE Primary
E- Safety Policy

Approved by:
Headteacher Mr D Jordan **Date:24.09.2025**
Chair of Governors Mrs Laura Gregory-White **Date:24.09.2025**
Review date: Autumn 2026

Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors;
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology;
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

Legislation and guidance

This policy is based on the Department for Education's (DfE) 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 and DfE's guidance on generative artificial intelligence in school

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.

Roles and responsibilities

The governing board

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

The governing board will meet with the designated safeguarding lead (DSL) to discuss online safety and monitor online safety logs.

All governors will:

- Ensure that they have read and understand this policy;
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet.

The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

The designated safeguarding lead (also the Headteacher at Thurgoland CE Primary)

Details of the school's DSL and deputies are set out in our child protection 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;
- Take lead responsibility for online safety and understanding the filtering and monitoring systems and processes in place;
- Working with the headteacher and other staff, as necessary, to address any online safety issues or incidents;
- 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 and filtering and monitoring;
- 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.
- The Headteacher, Data Protection Officer and staff need to work together to understand emerging safeguarding risks related to AI in order to take action to protect the students in their care. The school needs to be prepared to respond to incidents when they occur, with student-generated images becoming increasingly common in cases of peer-on-peer harm.
- The school also needs to prepare specifically for recognising and responding to incidents related to generative AI.

This list is not intended to be exhaustive.

IT Provider

The IT provider Trust IT is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material and material produced by Artificial Intelligence;
- 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 fortnightly basis;
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files.

All staff and volunteers

All staff, including contractors 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 and ensuring that pupils follow the school's terms on acceptable use (see staff code of conduct);
- Working with the DSL to ensure that any online safety incidents are logged using CPOMS 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.

This list is not intended to be exhaustive.

Parents

Parents 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 school's ICT systems and internet (appendix 1).

Parents 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 International
- Parent factsheet - Childnet International
- Healthy relationships – Disrespect Nobody

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 (appendix 1).

Educating pupils about online safety

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

In **Key Stage 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 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;*
- *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.

Educating parents about online safety

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents.

Online safety will also be covered during parents' information evenings.

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

Concerns or queries about this policy can be raised with any member of staff or the headteacher.

Cyber-bullying

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 one person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

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.

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 staff, 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 so that 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 consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Acceptable use of the internet in school

All pupils, parents, staff and volunteers are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet.

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 and staff, volunteers.

The Headteacher, Mr D Jordan, alongside Mrs L Hoyland, Safety Governor, are responsible for ensuring that filtering and monitoring standards are met. Gareth Wood, Trust IT, works closely with the Headteacher to ensure that the school meets the Department for Education's new filtering and monitoring standards (DfE, 2023b).

Online safety, the use of mobile technology and filtering and monitoring

We recognise the importance of safeguarding children from potentially harmful and inappropriate online material, and we understand that technology is a significant component in many safeguarding and wellbeing issues.

To address this, our school aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, volunteers and governors.
- Protect and educate the whole school community in its safe and responsible use of technology, including mobile and smart technology (which we refer to as 'mobile phones').
- Set clear guidelines for the use of mobile phones for the whole school community.
- Establish clear mechanisms to identify, intervene in and escalate any incidents or concerns, where appropriate.
- Have an appropriate filtering and monitoring system in place and regularly review their effectiveness.

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, anti-Semitism, radicalisation, extremism disinformation, misinformation and conspiracy theories.

  **Disinformation is the deliberate creation and spread of false or misleading content, such as fake news. Misinformation is the unintentional spread of this false or misleading content (Cabinet Office, Department for Science, Innovation and Technology, 2023). **
- **Contact** – being subjected to harmful online interaction with other users, such as child-to-child 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.
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

To meet our aims and address the risks above we will:

- Educate pupils about online safety as part of our curriculum. For example:
    - The safe use of social media, the internet and technology.
    - Keeping personal information private.
    - How to recognise unacceptable behaviour online.
    - How to report any incidents of cyber-bullying, ensuring pupils are encouraged to do so, including where they are a witness rather than a victim.
- Train staff, as part of their induction, on safe internet use, online safeguarding issues including cyber-bullying and the risks of online radicalisation and on their responsibilities to understand filtering / monitoring systems. All staff members will receive refresher training at least once each academic year.
- Educate parents/carers about online safety via our website, communications sent directly to them and during parents' evenings. We will also share clear procedures with them so they know how to raise concerns about online safety.
- Make sure staff are aware of any restrictions placed on them with regards to the use of their mobile phone and cameras, for example that:

- Staff are allowed to bring their personal phones to school for their own use, but will limit such use to non-contact time when pupils are not present.
- Staff will not take pictures or recordings of pupils on their personal phones or cameras.

- Make all pupils, parents/carers, staff, volunteers and governors aware that they are expected to sign an agreement regarding the acceptable use of the internet in school, use of the school's ICT systems and use of their mobile and smart technology.
- Pupils are not allowed to use mobile phones on the school premises. When pupils bring phones to school, they will be switched off, handed to a member of staff and kept in the school safe until the end of the day.
- Explain the sanctions we will use if a pupil is in breach of our policies on the acceptable use of the internet and mobile phones.
- Make sure all staff, pupils and parents/carers are aware that staff have the power to search pupils' phones, as set out in the DfE's guidance on searching, screening and confiscation.
- Put in place robust filtering and monitoring systems to limit children's exposure to the 4 key categories of risk (described above) from the school's IT systems.
- Carry out an annual review of our approach to online safety, supported by an annual risk assessment that considers and reflects the risks faced by our school community.

The Headteacher, Mr D Jordan, alongside Mrs L Hoyland, Safety Governor, are responsible for ensuring that filtering and monitoring standards are met - including Generative Ai: product safety expectations in line with DfE guidance -Gareth Wood, Trust IT, works closely with the Headteacher to ensure that the school meets the Department for Education's new filtering and monitoring standards (DfE, 2023b).

The senior leadership team are responsible for:

- procuring filtering and monitoring systems
- documenting decisions on what is blocked or allowed and why
- reviewing the effectiveness of your provision
- overseeing reports

They are also responsible for making sure that all staff:

- understand their role
- are appropriately trained
- follow policies, processes and procedures
- act on reports and concerns

The IT service provider should work with the senior leadership team and DSL to:

- procure systems
- identify risk
- carry out reviews
- carry out checks

A review of filtering and monitoring at Thurgoland CE Primary is carried out annually – or when there is a safeguarding risk or new technology is introduced - to identify our current provision, any gaps, and the specific needs of our pupils and staff.

The following content is checked:

- the risk profile of your pupils, including their age range, pupils with special educational needs and disability (SEND), pupils with English as an additional language (EAL)
- what your filtering system currently blocks or allows and why
- any outside safeguarding influences, such as county lines
- any relevant safeguarding reports
- the digital resilience of your pupils
- teaching requirements, for example, your RHSE and PSHE curriculum
- the specific use of your chosen technologies, including Bring Your Own Device (BYOD)
- what related safeguarding or technology policies you have in place
- what checks are currently taking place and how resulting actions are handled

To make our filtering and monitoring provision effective, our review informs:

- related safeguarding or technology policies and procedures
- roles and responsibilities
- training of staff
- curriculum and learning opportunities
- procurement decisions
- how often and what is checked
- monitoring strategies

This section summarises our approach to online safety and mobile phone use. For comprehensive details about our school's policy on online safety and the use of mobile phones, please refer to our online safety policy and mobile phone policy, which you can find on our website.

Pupils using mobile devices in school

Any pupils bringing mobile phones into school will be required to leave them in the school office. They will be kept in a secure location and returned at the end of the day.

Staff using work devices outside school

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);
- Ensuring their 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 – Trust IT will ensure this is in place;
- 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- Trust IT will provide this;
- Keeping operating systems up to date – always install the latest updates;
- Staff use approved Artificial Intelligence in line with the school's Artificial Intelligence platform;
- Staff members must not use the device in any way which would violate the school's code of conduct;
- If staff have any concerns over the security of their device, they must seek advice from the school's IT provider Trust IT.

How the school will respond to issues of misuse

Where a pupil misuses the school'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 staff member 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 disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

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

All staff members 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).

The DSL and deputy will undertake child protection and safeguarding training, which will include online safety, at least every 3 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.

Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety using CPOMs.

The Headteacher and Deputy Headteacher receive, via email, filtering and monitoring breach reports.

This policy will be reviewed every year by the head teacher.

13. Links with other policies

This online safety policy is linked to our:

- Child protection and safeguarding policy;
- Behaviour and Relationships Policy;
- Staff disciplinary procedures;
- Data protection policy and privacy notices;
- Complaints procedure;
- ICT and internet acceptable use policy;
- Bring Your Own Device Policy;
- Staff Code of Conduct;
- Artificial Intelligence Policy.

Appendix 1: Acceptable use agreement (pupils and parents/carers)

Thurgoland CE Primary Pupils' E-safety Agreement

For my own personal safety

- I will ask permission from a member of staff before using the Internet at school.
- I am aware of "stranger danger" when on line and will not agree to meet online friends.
- I will tell an adult about anything online which makes me feel uncomfortable.
- I will only use a webcam with people I know and with the approval and consent of a parent/carer first.
- I understand that the school may check my files and may monitor the web pages I visit.
- When in school I will only contact people with my teacher's permission.
- I will be very careful when sharing pictures or video of myself, my friends or my family. If I am in school, I will always check with a teacher. If I am at home, I will check with my parents.
- I will not put my "personal information" online. (My full name, birthday, phone number, address, postcode, school etc.)
- I will only use child friendly search engines
- I will always follow the SMART rules of e-safety

To keep the system safe

- I will only use my own login and password, which I will keep secret.
- I will not access other people's files.
- I will not play games on a school computer unless my teacher has given me permission.
- I will not install software on school computers.
- I will not use the system for gaming, shopping, or uploading videos or music.

Responsibility to others

- The messages I send will be polite and responsible.
- I will not upload images or video of other people without their permission.
- Where work is copyrighted (including music, videos and images,) I will not either download or share with others.
- I understand that the school may take action against me if I am involved in inappropriate behaviour on the internet and mobile devices.

Personal Devices

- The school cannot accept responsibility for loss or damage to personal devices.

- It is not permitted for pupils to use mobile phones during the school day. Phones should not be brought into school unless there is a genuine reason for doing so and my parents have approved this. If I have to bring my phone into school, I will hand it into my teacher at registration and get it back at the end of the school day.
- Other devices (e.g. Games consoles, cameras) should not be brought into school.

Further information for parents:
Children will receive advice on e-safety at school, advice for parents is available at www.thinkuknow.org.uk/parents or by contacting the school.
Please inform the school if you have concerns over your child's e-safety.
Ensure that any pictures or videos taken during school events that include other children are not shared using social media.