THE SPIRE
CHURCH OF ENGLAND LEARNING TRUST

collaborate . learn . achieve

The Spire Church of England Learning Trust

Online Safety and Acceptable Use Policy 2025 – 2027

This policy is reviewed and updated by one of the Trust Headteachers. It is approved on a biennial basis by the Trust Board and implemented by all schools within the Trust.

This document will be subject to an ongoing review. It may be amended prior to the scheduled date of the next review in order to reflect changes in legislation where appropriate.

Reviewed:	January 2025
Ratified:	February 2025
Next Review Date:	January 2027

Version 2

In collaboration with

Introduction

This policy has been written in conjunction with the following:

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

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

This policy complies with our funding agreement and Articles of Association.

1. Aims

The Spire Church of England Learning Trust aims to:

- Have robust processes in place to ensure the online safety of pupils, staff, 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, for example: pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories.
- **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** – 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. If you feel your pupils, pupils or staff are at risk, please report it to the Anti-Phishing Working Group https://apwg.org/

2. Roles and Responsibilities

School Data Protection Co-ordinator- this role differs to the Data Protection Officer (DPO) which is carried out by SchoolPro TLC Limited

The authorised CCTV system operators in each school within the Trust are:

- Headteacher/Head of School
- All members of the Senior Leadership Team
- Site Manager/Caretaker
- School Network Manager/Technician and Trust IT Manager

Each school within the Trust have the following staff who are authorised to make requests to view CCTV data:

- Heads of KS/Year
- Pastoral Leaders
- All members of the Senior Leadership Team

Parents/Carers:

Under the UK GDPR, individuals have the right to obtain confirmation that their personal information is being processed. All disks containing images belong to, and remain the property of the school.

Individuals have the right to submit an SAR (Subject Access Request) to gain access to their personal data in order to verify the lawfulness of the processing. The school will verify the identity of the person making the request before any information is supplied.

A copy will be provided free of charge. However, in line with UK GDPR and ICO guidance, the Trust may charge a reasonable fee based on administrative costs where a request is manifestly unfounded or excessive, or for further copies of the same information.

Contact Details List

St John's CE Middle School
office@st-johns-bromsgrove.worcs.sch.uk
Tel : 01527 832376

St John's CE Primary School
office@stjohns.worcs.sch.uk
Tel : 01562 745558

St Matthias CE Primary School
admin@stmatthias.worcs.sch.uk
Tel : 01684 574984

Witton Middle School
office@witton.worcs.sch.uk
Tel : 01905 773362

Catshill First School and Nursery
office@catshillfirst.worcs.sch.uk
Tel : 01527 872913

Catshill Middle School, Bromsgrove
office@catshill-middle.worcs.sch.uk
Tel : 01527 872431

2.1 The Directors and Governing Boards

The Directors have overall responsibility for monitoring this policy and holding the Headteacher/Head of School to account for its implementation.

The Local 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 Local Governing Board will also make sure 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 Local 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 Local Governing Board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The Local 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 the 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 Local Governor who oversees online safety is the Safeguarding Governor of the school.

All Governors will:

- Ensure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's IT systems and the internet (appendix 3)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- 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.

2.2 The Headteacher/Head of School

The Headteacher/Head of School is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

2.3 The Designated Safeguarding Lead (DSL)

Details of the school's designated safeguarding lead (DSL) and 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/Head of School in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Working with the Headteacher/Head of School and Local 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 IT Manager to make sure the appropriate systems and processes are in place
- Working with the Headteacher/Head of School, IT 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 (see appendix 5) 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 (appendix 4 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/Head of School and/or Local 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
- Ensuring the Trust completes the "DfE Plan technology for your school" self assessment for filtering and monitoring at least annually and after any material change, and that resulting actions are implemented and reported to senior leaders and governors.

This list is not intended to be exhaustive.

2.4 The IT Manager/Network Manager

The IT 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 IT 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 IT systems on a 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 (see appendix 5) 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

- Implementing and maintaining filtering and monitoring controls that address AI-generated and real-time content risks and preventing circumvention (e.g. VPNs or proxies) across school-managed devices and personal (BYOD) devices accessing school networks.
- Enforcing illegal content blocklists (e.g. child sexual abuse material and terrorism content) at all times with no opt-out, and documenting technical limitations or residual risks for DSL and leadership oversight.

This list is not intended to be exhaustive.

2.5 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 IT systems and the internet (appendix 3), and ensuring that pupils follow the school's terms on acceptable use (appendices 1 and 2)
- 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 liaising with the Network Manager and talking to pupils and parents/carers as appropriate.

- Following the correct procedures by making a request to the Network Manager 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 (see appendix 5) 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'
- Following procedures for the safe use of images as follows:
    - Creation of videos and photographs

      With the consent of parents/carers (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment. Staff are not permitted to use personal devices, such as mobile phones or tablets to record images of pupils. The school's own mobile devices must be used.
    - Publishing pupil's images and work

      Parents/carers will be asked to give permission for the school to use their child's work/photos in publicity materials or on the school website or social media outlets. The consent form is deemed valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue. Parents/carers may withdraw or amend permission, in writing, at any time. Pupils' full names will not be published alongside their image or vice versa on school-based publicity materials.
    - Storage of images

      Images/films of children are stored securely on the school server and/or teacher's individual encrypted devices for the length of time the pupil remains at the school.

This list is not intended to be exhaustive.

2.6 Parents/Carers

Parents/carers are expected to:

- Notify a member of staff or the Headteacher/Head of School 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 IT systems and internet (appendices 1 and 2)

Parents/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/Carer resource sheet – Childnet

2.7 Visitors and Members of the Community

Visitors and members of the community who use the school's IT 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 3).

3. Educating Pupils about Online Safety

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

The text below is taken from the National Curriculum computing programmes of study.

It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary 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 KS2**, 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

In **KS3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- Recognise inappropriate content, contact and conduct, and know how to report concerns

By the **end of KS3**, pupils will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online
- Not to provide material to others that they would not want shared further and not to share personal material that is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted pITure of sexual behaviours, can damage the way people see themselves in relation to others, and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours

- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)
    - The Trust will review and, where appropriate, update its RSHE and online safety curriculum to reflect the revised statutory RSHE guidance published in December 2025, to be implemented by 1 September 2026 (with earlier adoption where feasible). This includes explicit content on AI deepfakes, online misogyny, and emerging online harms.

The safe use of social media and the internet will also be covered in other subjects where relevant, for example, PSHE. Children will be taught how to report issues and how to seek advice.

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, vITims of abuse and some pupils with SEND.

4. Educating Parents/Carers about Online Safety

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

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

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

Concerns or queries about this policy can be raised with any member of staff or the Headteacher/Head of School.

5. Cyber-Bullying

5.1 Definition

We recognise that child on child abuse and child on child sexual violence and sexual harassment can occur online. 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.)

5.2 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 vITim.

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/form teachers will discuss cyber-bullying with their tutor groups.

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 (see section 11 for more detail).

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.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour and/or anti-bullying 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.

5.3 Examining Electronic Devices

The Headteacher/Head of School, and any member of staff authorised to do so by the Headteacher/Head of School (as set out in the School's Behaviour Policy) can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff 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

- These powers reflect the Education Act 2011 (Part 2), which permits authorised staff to examine data or files on an electronic device where there is a good reason to do so. Staff may erase data or files if they believe there is a good reason, unless the data is suspected to be evidence relevant to an offence or a safeguarding incident.

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 staff. If the search is not urgent, they will seek advice from the Headteacher/Head of School.
- 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 staff member 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 the staff member in conjunction with the DSL / Headteacher / Head of School to decide on a suitable response. If there are images, data or files on the device that staff 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, staff members 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/carer refuses to delete the material themselves

If a staff member **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 equivalent) 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
- The school's 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.

Staff must act in line with KCSIE and the DfE guidance on 'Searching, Screening and Confiscation', ensuring that all decisions and actions taken are formally recorded

5.4 Artificial Intelligence (AI)

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

The Trust 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 Trust will treat any use of AI to bully pupils in line with our Anti-Bullying/Behaviour Policy.

Pupils in schools within the Trust are permitted to use AI tools in school on school devices under staff supervision. Staff may also use AI tools to assist with workload. However,.staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school.

Children will be taught about the benefits and disadvantages of AI and how to use it safely and honestly. Staff will be alert to AI being used by pupils to complete homework tasks and projects and discourage pupils from using AI dishonestly.

Please see Appendices 6, 7 and 8 for risk assessment and additional checklists.

6. Acceptable Use of the Internet in School

All pupils, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's IT systems and the internet (appendices 1 to 3). 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, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate. We will monitor internet usage by pupils, staff, volunteers, governors, and visitors (where relevant) to ensure compliance with the above, and restrict access to inappropriate content through filtering systems. This applies to all devices that access school networks or services, whether school-managed or personal devices (BYOD).

More information is set out in the acceptable use agreements in appendices 1 to 3.

7. Pupils Using Mobile Devices in School

Please see the school's Mobile Devices Policy. Any use of mobile devices in school by pupils must be in line with the acceptable use agreement (see appendices 1 and 2).

Any breach of the 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.

Where personal (BYOD) devices connect to school networks or services, they are subject to the same filtering and monitoring controls as school-managed devices. The use of VPNs, proxies, or other methods to bypass safety controls is strictly prohibited and will be actively prevented and addressed.

8. 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
- 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, as set out in appendix 3.

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 IT Manager.

9. How the School Will Respond to Issues of Misuse

Where a pupil misuses the school's IT systems or internet, we will follow the procedures set out in our policies on behaviour and IT 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 IT 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 / staff code of conduct. 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.

10. Training

All new staff members 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 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).

By way of this training, all staff 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 staff:

- 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, at least every 2 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.

11. Monitoring Arrangements

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

To evidence compliance with Keeping Children Safe in Education (KCSIE) and the DfE Filtering and Monitoring Standards, the Trust will:

(i) Record an annual filtering and monitoring review

(ii) Complete the DfE 'Plan technology for your school' self-assessment, including an action plan; and

(iii) Minute leadership and governor oversight in safeguarding reports.

Reviews will explicitly consider AI-related risks and the practical effectiveness of controls, rather than just their design.

This policy will be reviewed every two years and will be approved by the Board of Directors. At every review, the policy will be shared and implemented by all schools within the Trust. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Appendix 1: EYFS and KS1 Acceptable Use Agreement (Pupils and Parents/Carers)

ACCEPTABLE USE OF THE SCHOOL'S IT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of Pupil:	

When I use the school's IT 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 IT 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 IT 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 IT systems and internet, and will make sure my child understands these.	
Signed (Parent/Carer):	**Date:**

Appendix 2: KS2, KS3 and KS4 Acceptable Use Agreement (Pupils and Parents/Carers)

ACCEPTABLE USE OF THE SCHOOL'S IT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS AND PARENTS/CARERS	
Name of Pupil:	
I will read and follow the rules in the acceptable use agreement policy. **When I use the school's IT systems (like computers) and get onto the internet in school I will:** • Always use the school's IT systems and the internet responsibly and for educational purposes only • Only use them when a teacher is present, or with a teacher's permission • Keep my usernames and passwords safe and not share these with others • Keep my private information safe at all times and not give my name, address or telephone number to anyone without the permission of my teacher or parent/carer • Tell a teacher (or sensible adult) immediately if I find any material that might upset, distress or harm me or others • Always log off or shut down a computer when I've finished working on it **I will not:** • Access any inappropriate websites including: social networking sites, chat rooms and gaming sites unless my teacher has expressly allowed this as part of a learning activity • Open any attachments in emails, or follow any links in emails, without first checking with a teacher • Use any inappropriate language when communicating online, including in emails • Create, link to or post any material that is pornographic, offensive, obscene or otherwise inappropriate • Log in to the school's network using someone else's details • Arrange to meet anyone offline without first consulting my parent/carer, or without adult supervision **If I bring a personal mobile phone or other personal electronic device into school:** • I will not use it during lessons, tutor group time, clubs or other activities organised by the school, without a teacher's permission • I will use it responsibly, and will not access any inappropriate websites or other inappropriate material or use inappropriate language when communicating online **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's agreement: I agree that my child can use the school's IT 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 IT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (Parent/Carer):	**Date:**

Appendix 3: Acceptable Use Agreement (Staff, Governors, Volunteers and Visitors)

ACCEPTABLE USE OF THE SCHOOL'S IT SYSTEMS AND INTERNET: AGREEMENT FOR STAFF, GOVERNORS, VOLUNTEERS AND VISITORS	
Name of Staff Member/Governor/Volunteer/Visitor:	
When using the school's IT 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 that could harm the school's reputation • Access social networking or chat platforms unless expressly approved for a legitimate educational purpose using a school-managed account, with professional conduct and monitoring controls in place. • 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 IT 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 IT 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 designated safeguarding lead (DSL) and IT Manager know if a pupil informs me they have found any material that 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 IT systems and internet responsibly, and ensure that pupils in my care do so too. I will not use social media groups/blogs, either in or out of school, to criticise, make offensive, defamatory, discriminatory or otherwise inappropriate comments about the school or Trust.	
Signed (Staff Member/Governor/Volunteer/Visitor):	**Date:**

Appendix 4: Online Safety Training Needs – Self-Audit for Staff

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name of Staff Member/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 IT 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 5: Online Safety Incident Report Log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**

Appendix 6: AI Tool Evaluation Checklist for School Leaders

This comprehensive checklist has been updated to reflect DfE Product Safety Expectations (June 2025) and safeguarding requirements.

Initial Assessment: Educational Purpose and Benefits

What educational benefit or improvement does this AI tool provide?

- Describe the specific educational outcome or improvement this tool will deliver
- Identify how it enhances teaching, learning, or administrative processes
- Explain why this particular solution is needed at this time

Target users and context:

- Who will use this tool? (Teachers only / Pupils only / Both)
- What age groups will it serve?
- Does it generate images or multimodal content?
- Will it be used on personal devices (BYOD) or school-managed devices only?

Notes:

Section 1: Safety and Security (Essential Requirements)

1.1 Content Safety *(Essential for child-facing products)*

- ☐ Tool blocks harmful/inappropriate content generation
- ☐ Age-appropriate filtering for your pupil age groups
- ☐ Filtering works across text, images, multiple languages
- ☐ Real-time content blocking with user explanations
- ☐ Filtering maintained on all devices (including BYOD)

Mark N/A if tool is teacher-only

1.2 Data Protection *(Applies to all tools)*

- UK GDPR compliant with clear privacy policy
- Explains what data is collected and how it's used
- States where data is processed (UK/EU preferred)
- Confirms data won't be used to train AI without consent
- Provides data deletion on request

1.3 Technical Security *(Applies to all tools)*

- ☐ Meets DfE Cyber Security Standards for Schools
- ☐ Strong password/authentication requirements
- ☐ Regular security updates and patches
- ☐ Administrative controls for user permissions

Section 2: Monitoring and Reporting *(Essential for child-facing products)*

2.1 Activity Monitoring

- ☐ Records user activity for safeguarding purposes
- ☐ Alerts school staff to harmful content attempts
- ☐ Provides real-time notifications when content blocked
- ☐ Identifies potential safeguarding disclosures

2.2 Reporting Capabilities

- ☐ Provides reports schools can understand and use
- ☐ Shows trends in content access attempts
- ☐ Has clear incident reporting procedures
- ☐ Formal escalation process for safety issues

Mark N/A if tool is teacher-only

Section 3: Educational Suitability *(Applies to all teacher tools)*

3.1 Curriculum Alignment

- ☐ Content aligns with UK National Curriculum
- ☐ Accurate for intended subjects and age groups
- ☐ Age-appropriate content and complexity
- ☐ Enhances rather than replaces meaningful learning
- ☐ Evidence of positive impact in schools

3.2 Pedagogical Considerations

- ☐ Supports rather than replaces teacher expertise
- ☐ Encourages critical evaluation of AI outputs
- ☐ Supports diverse learning needs and abilities
- ☐ Compatible with existing assessment practices
- ☐ Provides useful feedback to educators

Mark N/A if tool is leadership-only

Section 4: Intellectual Property Protection *(Applies to all tools)*

4.1 Copyright and Creative Work Protection

- ☐ Pupil work protected from unauthorised use
- ☐ Teacher work protected from unauthorised use
- ☐ Clear consent processes for any data use
- ☐ Parental consent for under-18 users where needed
- ☐ No commercial use of inputs/outputs without permission
- ☐ Clear opt-out from any AI training

4.2 Content Attribution and Copyright

- ☐ AI-generated content clearly identified
- ☐ Measures to prevent copyright infringement
- ☐ Clear content ownership and usage rights
- ☐ Respects employer copyright in teacher-created works

Section 5: Transparency and Accountability *(Applies to all tools)*

5.1 Explainability and Openness

- ☐ Information about training data sources
- ☐ Clear explanation of tool limitations
- ☐ Acknowledges and addresses potential biases

5.2 Provider Accountability

- ☐ Provider demonstrates education sector understanding
- ☐ UK regulatory compliance
- ☐ Responsive technical and educational support
- ☐ Regular updates and improvement processes
- ☐ Formal complaints and escalation procedures

Section 6: Design and Testing *(Applies to all tools)*

6.1 User-Centred Design

- ☐ Child-centred design prioritising safety *(for child-facing tools)*
- ☐ Meets accessibility and SEND requirements
- ☐ Performs consistently as intended
- ☐ Design eliminates discrimination and bias where reasonably possible

6.2 Safety Testing and Validation

- ☐ Input from educators and pupils (child-facing products) in development
- ☐ Technical safeguards for identified risks
- ☐ Ongoing improvement based on user feedback
- ☐ Regular assessment of safety and effectiveness

Section 7: Implementation and Support *(Applies to all tools)*

7.1 Technical and Educational Support

- ☐ Responsive technical support available
- ☐ Guidance on educational implementation
- ☐ Comprehensive training programmes

7.2 Change Management and Integration

- ☐ Considers staff capacity and skills
- ☐ Plans for communicating changes
- ☐ Mechanisms to gather user feedback

Section 8: Cost and Sustainability *(Applies to all tools)*

8.1 Financial Considerations

- ☐ Clear educational benefits justify cost
- ☐ All costs transparent (no hidden fees)
- ☐ Affordable within school budget
- ☐ Good value compared to alternatives
- ☐ Potential for measurable return on investment

Scoring and Decision Framework

Scoring Instructions:

□ Yes - Requirement fully met	□ No - Requirement not met	- N/A - Not applicable to this tool

Essential Requirements (Must all be "Yes"):

For Child-Facing Tools:

- All Section 1 (Safety and Security) applicable items
- All Section 2 (Monitoring and Reporting) items
- All Section 4 (Intellectual Property) items

For Teacher-Only Tools:

- Section 1.2 and 1.3 (Data Protection and Technical Security)
- All Section 4 (Intellectual Property) items

Recommended Standards:

- Child-facing tools: 90%+ of all applicable items should be "Yes"
- Teacher-only tools: 85%+ of all applicable items should be "Yes"

Total Applicable Items:	_____
Items Scoring "Yes":	_____
Percentage:	_____%

Evaluator Information:

Name: _____

Role: _____

Review Date:

Final Recommendation:

□ Approve for implementation - All essential criteria met, benefits clear

□ Conditional approval - Approve with specific conditions or limitations

□ Further evaluation needed - Requires additional assessment or information

□ Reject - Does not meet essential requirements

Key Conditions/Actions Required:

Appendix 7: AI Implementation Plan Template

Use this template to plan the implementation of a new AI tool in your school.

1. Tool Information

Name of AI Tool:	
Purpose:	
Provider:	

2. Implementation Timeline

Start Data:	
Pilot Phase Duration:	
Full Implementation Date:	

3. Stakeholder Communication Plan

Stakeholder Group	Communication Method	Frequency	Responsible Person
Staff			
Pupils			
Parents/Carers			
Governors			

4. Training Plan

Objective	Training Details	Audience	Trainer	Success Criteria

5. Evaluation

Purpose:
Evaluation:

Appendix 8: Staff AI Safety Quick Reference Guide

This quick reference guide provides essential safety information for all staff using AI tools in educational settings.

🚨 Essential Safety Rules

❌ NEVER Do These Things:

- Input personal data into **unapproved** AI tools or free personal AI accounts
- Use free, consumer AI tools (ChatGPT, Gemini, etc.) for school work involving personal data
- Upload pupil work to unapproved tools without proper permissions and safeguards
- Share AI-generated content without checking for accuracy and appropriateness
- Allow unsupervised pupil access to AI tools without proper safeguards
- Rely solely on AI outputs without human verification
- Use AI for final decisions about pupils without human review

✅ ALWAYS Do These Things:

- Use only approved AI tools provided by the school
- Verify that approved tools have appropriate data protection measures (e.g., no model training on user data)
- Check all AI outputs for accuracy, bias, and appropriateness
- Maintain human oversight of all AI-assisted work
- Report concerns immediately to DSL or senior leadership
- Follow data protection guidelines when using any AI tool
- Be transparent about AI use with pupils and colleagues
- Keep learning about AI developments and best practices

🔍 Recognising AI Limitations

Watch Out For:

- **Hallucinations:** AI making up convincing but false information
- **Bias:** Unfair representation of groups or individuals
- **Outdated information:** AI training data may be months or years old
- **Context misunderstanding:** AI may not grasp local or specific situations
- **Inappropriate content:** Despite filters, concerning content may occasionally appear

Red Flags in AI Outputs:

- Unusual facts without sources
- Content that seems "too good to be true"
- Stereotypical representations
- Inconsistent information
- Overly complex or simple language for the context

📊 Data Protection Quick Check

Before Using Any AI Tool, Ask:

- Is this tool approved by our school?
- Does this tool have appropriate data protection measures in place?
- If using personal data, is this tool specifically approved for such use?
- Could this data be used to train the AI model inappropriately?
- Do I have permission to use any copyrighted content?
- Is there a non-AI way to accomplish this task?

Understanding Tool Categories:

✅ **Approved tools with data protection** (e.g., school MIS system with AI features, enterprise AI tools with no-training policies etc):

- May be used with personal data as per school policy
- Still require appropriate professional judgement
- Must follow any specific usage guidelines

⚠️ **Approved tools without data protection** (general AI tools):

- Use placeholder names (e.g., "Pupil A," "The teacher")
- Remove identifying details from any text
- Anonymise data before inputting

❌ **Unapproved tools:**

- Never use for school work
- Never input any school-related data

🛡️ Safeguarding Checklist

If You Encounter Concerning Content:

- Don't panic - take a screenshot if safe to do so
- Stop using the tool immediately
- Report to DSL or senior leadership
- Document what happened and what you were trying to do
- Follow normal safeguarding procedures

Warning Signs to Report:

- Generation of inappropriate images or text
- Content that could be used for grooming or exploitation
- Discriminatory or hateful outputs
- Content promoting harmful activities
- Any output that raises safeguarding concerns

🎓 Academic Integrity Guidelines

When Working with Pupils:

- Be clear about when AI use is/isn't appropriate
- Teach pupils to identify AI-generated content
- Model critical evaluation of AI outputs
- Emphasise the importance of human thinking and creativity
- Check work for signs of AI assistance when inappropriate

Signs of Potential AI Misuse in Pupil Work:

- Sudden improvement in writing quality
- Unusual vocabulary or writing style
- Lack of personal voice or perspective
- Perfect grammar in otherwise inconsistent work
- References or information that seem out of place

🤝 Getting Help and Support

Who to Contact:

Issue Type	Contact	When
Technical problems	IT Support	During work hours
Safeguarding concerns	DSL	Immediately
Data protection questions	DPO	Before using new tools
Training needs	Line Manager	Ongoing
General AI questions	AI Lead/Senior Leader	Any time

Resources Available:

- DfE AI Toolkit Modules (mandatory for all staff)
- School AI Policy (available on staff intranet)
- Regular CPD sessions on AI use
- Peer support networks within school
- External training opportunities as available

📝 Quick Decision Tree

Thinking of using AI? Follow this process:

1. **Is this an approved tool?** → If NO, stop here
2. **Do I need to input personal data?** → If YES, check it's approved for personal data use
3. **Will this enhance rather than replace my professional judgement?** → If NO, reconsider
4. **Can I check and verify the output?** → If NO, don't use
5. **Is this transparent and ethical?** → If NO, find another approach

6. **Will this genuinely save time or improve outcomes?** → If YES, proceed with caution

🔄 Regular Review Questions

Ask yourself monthly:

- Am I using AI tools safely and effectively?
- Have I kept up with training and policy updates?
- Am I modelling good AI practices for pupils?
- Are there new AI-related risks I should be aware of?
- Do I need additional support or training?

Remember: AI is a tool to enhance human expertise, not replace it. When in doubt, ask for help!