ST THOMAS AQUINAS
CATHOLIC MULTI-ACADEMY TRUST

ST THOMAS AQUINAS

Catholic Multi-Academy Trust

ONLINE SAFETY POLICY

DATE OF ADOPTION	22 September 2025
ADOPTED BY	Trust Board
REVIEW DATE	May 2027

Online Safety Policy – Review 2025

The Online Safety Policy has been reviewed and updated in line with DfE statutory guidance for 2025, including *Keeping Children Safe in Education*, the *Filtering and Monitoring Standards*, and the *Generative Artificial Intelligence in Education* guidance. Key changes are outlined below.

The policy now includes a dedicated section on Generative AI, setting clear expectations for safe and ethical use, requiring risk assessments before adoption, providing staff training and pupil education on opportunities, risks, and misinformation, and ensuring AI is never used to bully, mislead, or make decisions about people without human oversight.

The policy introduces a clear step-by-step incident pathway, defining reporting routes to the DSL, setting out their responsibilities, establishing escalation to the Trust Safeguarding Director or external agencies, requiring governor oversight and trend analysis, and ensuring appropriate support for victims and perpetrators.

The policy now includes a dedicated section on SEND and vulnerable pupils, requiring adapted online safety education, staff training on specific risks, use of individual risk assessments and accessible reporting routes, targeted parental support, and DSL oversight, ensuring safeguarding is personalised and fully compliant with KCSIE.

Contents

1. Aims
2. Legislation and guidance
3. Roles and responsibilities
4. Educating pupils about online safety
5. Educating parents/carers about online safety
6. Cyber-bullying
7. Acceptable use of internet in school
8. Artificial intelligence
9. SEND, Vulnerable Pupils and Tailored Online Safety
10. Pupils using mobile devices in school
11. Staff using work devices outside school
12. How the school will respond to issues of misuse
13. Training
14. Monitoring arrangements
15. Links with other policies

Appendix 1: EYFS and KS1 acceptable use agreement (pupils and parents/carers)

Appendix 2: KS2, KS3 and KS4 acceptable use agreement (pupils and parents/carers)

Appendix 3: acceptable use agreement (staff, governors, volunteers and visitors)

Appendix 4: online safety training needs – self-audit for staff

Appendix 5: online safety incident report log

---

1. Aims

Our schools 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, 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 complies with our funding agreement and articles of association.

This policy has due regard to relevant legislation and statutory guidance, including:

- Online Safety Act 2023
- UK GDPR and Data Protection Act 2018
- Education Acts 1996, 2006, 2011
- Equality Act 2010
- Voyeurism (Offences) Act 2019
- DfE (2025) Keeping Children Safe in Education
- DfE Filtering and Monitoring Standards for Schools and Colleges (2025)
- DfE (2023) Teaching Online Safety in School
- DfE Preventing and Tackling Bullying (including cyberbullying)
- DfE Searching, Screening and Confiscation (2022)
- DfE (2025) Generative Artificial Intelligence in Education
- UKCIS Education for a Connected World (2020)
- National Cyber Security Centre guidance

3. Roles and responsibilities

a. The Board of Directors/ Local Governing Bod (LGB)

The Trust Board has overall responsibility for this policy. The LGB is responsible for monitoring and holding the headteacher to account for its implementation.

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

The Trust 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 Director of Business Services will, working with the Trust IT manager, make sure the appropriate systems and processes are in place

The Director of Safeguarding will co-ordinate regular meetings with appropriate staff to discuss online safety and requirements for training.

The LGB will monitor online safety logs as provided by the designated safeguarding lead (DSL).

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

The Trust Board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks and will consult with the Trust IT Manager to regularly review their effectiveness. The Trust 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 those 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.

All directors/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

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.

b. The headteacher

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

c. The designated safeguarding lead

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 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 headteacher, Trust IT manager/ Technology Support Manager and other staff, as necessary, to address any online safety issues or incidents

Taking the lead on checking the filtering and monitoring

Managing all online safety issues and incidents in line with the school's child protection policy

Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy

Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy

Updating and delivering staff training on online safety

Liaising with other agencies and/or external services if necessary

Providing regular reports on online safety in school to the headteacher and/or governing board

Undertaking annual risk assessments that consider and reflect the risks children face

Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

d. The Trust IT manager

Working with the Director of Business Services, the Trust IT Manager is responsible for:

Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on all school devices and the Trust network, 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 all IT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly

Conducting a full security check on a weekly basis

Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy

This list is not intended to be exhaustive.

e. 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, and ensuring that pupils follow the school's terms on acceptable use

Knowing that the DSL is responsible for filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing

Following the correct procedures 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.

f. Parents/carers

Parents/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 school's IT systems and internet

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 International

Parent resource sheet – Childnet International

g. 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.

4. 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 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

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 **Key Stage 3**, 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 Pupils in **Key Stage 4** will be taught:

To understand how changes in technology affect safety, including new ways to protect their online privacy and identity

How to report a range of concerns

By the **end of secondary school**, 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 which 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 picture 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 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/carers about online safety

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

Where possible online safety will also be covered during parents'

evenings. 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 and/or the DSL.

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

6. Cyber-bullying

a. 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.)

b. 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/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, LGB 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 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.

c. 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 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

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 / 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 in conjunction with the DSL 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 Headteacher in conjunction with the DSL / other member of the senior leadership team 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 in conjunction with the DSL 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

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

7. 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. 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.

The Trust IT team 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.

8 Artificial intelligence (AI)

Generative Artificial Intelligence (AI) tools are now widespread and easy to access. Staff, pupils, and parents/carers may already be familiar with tools such as ChatGPT, Google Bard, and other text, image, or video generators. The Trust recognises that AI can be a powerful resource to support learning, creativity, and efficiency. However, it also carries risks, and its misuse can cause harm.

AI must never be used to bully, harass, or mislead others. This includes the creation or sharing of 'deepfakes', where AI is used to generate false images, audio, or video content that may cause harm, embarrassment, or reputational damage. Such misuse may involve deepfake pornography or other offensive material created using someone's likeness without their consent. Any such behaviour will be treated in line with the Trust's Anti-Bullying and Behaviour policies, and where appropriate, reported to external authorities.

Staff must also recognise the risks of using AI tools whilst they remain under development. All new or proposed uses of AI within the school or Trust should be subject to a risk assessment, considering safeguarding, data protection, accuracy, and ethical implications. AI systems must never be used to make decisions about pupils or staff without appropriate human oversight and verification. Any AI-generated content used in teaching, administration, or communication must be carefully checked for accuracy, fairness, and suitability before being shared.

Personal, confidential, or sensitive information must never be input into AI systems unless expressly approved and in line with data protection regulations. Staff, pupils, and parents/carers should be made aware that AI outputs may be inaccurate, biased, or misleading, and should always be critically evaluated.

The Trust will continue to monitor developments in AI technology and review this policy regularly to ensure safe, ethical, and responsible use across all areas of school life.

In line with the DfE Generative Artificial Intelligence in Education (2025) guidance, the Trust is developing training for all **staff** on the safe, ethical, and effective use of AI tools. This will include:

- Understanding the opportunities and risks of AI in education (e.g. supporting learning, administration, and creativity).
- Recognising the dangers of misuse, including deepfakes, disinformation, bias, and breaches of data protection.
- Ensuring AI outputs are critically evaluated for accuracy, fairness, and appropriateness before

being used or shared.

- Knowing that AI systems must not be used to make decisions about pupils or staff without appropriate human oversight.
- Following school and Trust procedures for risk assessment and approval before introducing new AI tools.

Training will be refreshed at least annually, with updates provided where there are significant technological or regulatory developments.

As part of our online safety education, **pupils** will also learn about the safe and responsible use of Artificial Intelligence (AI) tools, in line with the DfE Generative Artificial Intelligence in Education (2025) guidance.

By the end of their time in school, pupils will understand that:

- AI tools (such as text, image, or video generators) can be helpful for learning and creativity, but they must be used critically and responsibly.
- AI systems sometimes produce information that is incorrect, biased, or misleading, so pupils must always check facts and seek guidance from trusted adults.
- AI must never be used to bully, embarrass, or deceive others, including creating "deepfakes" or false content that could cause harm.
- Personal, sensitive, or private information should never be entered into AI systems without permission, to keep themselves and others safe.
- Decisions about people (including pupils or staff) should never be left to AI tools without proper human oversight.

These lessons will be delivered through the computing curriculum, PSHE, RSE/health education, and other subjects where appropriate, and will be adapted for vulnerable pupils and those with SEND to ensure accessibility.

9. SEND, Vulnerable Pupils and Tailored Online Safety

The Trust recognises that some pupils are more vulnerable to online risks than others, particularly:

- Pupils with special educational needs and/or disabilities (SEND)
- Looked-after children (LAC) and care leavers
- Young carers
- Pupils experiencing mental health challenges
- Pupils who have experienced abuse, neglect or trauma

In line with *Keeping Children Safe in Education (2025)*, safeguarding and online safety teaching will be differentiated and tailored to meet the needs of these groups. A one-size-fits-all approach will not be used. This means:

- Online safety lessons will be adapted for accessibility, using visual supports, simplified language, additional adult support, or alternative resources where required.
- Staff will receive training on how to identify additional vulnerabilities to online grooming, exploitation, cyberbullying, and radicalisation in these groups.
- Pupils with communication difficulties will be supported to develop safe ways to report concerns using accessible methods (e.g. symbols, assistive technology, or trusted adults).
- Where appropriate, individual risk assessments will be completed for pupils whose vulnerabilities

increase the likelihood of online harm.

- Parents/carers of vulnerable pupils will be offered targeted support and resources to help them reinforce safe online behaviours at home.

The DSL will ensure that all teaching and safeguarding strategies take into account the individual needs of pupils, and that interventions are personalised, contextualised, and regularly reviewed.

10. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but are not permitted to use them in school including during: Lessons, Lunch and break time, Tutor group time, Clubs before or after school, or any other activities organised by the school.

Any use of mobile devices in school by pupils must be in line with the acceptable use agreement.

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.

11. 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)
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Staff members must not use the device in any way that would violate the school's terms of acceptable use. Staff devices are monitored at all times (on site and during use off site).

If staff have any concerns over the security of their device, they must seek advice from the Trust IT Manager.

12. 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. 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 and staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

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

Incident Reporting and Escalation Pathway

All members of the school community (staff, pupils, parents/carers, visitors) are expected to report online safety concerns immediately.

Step 1 – Initial Report

- Pupils: report to a trusted adult (teacher, tutor, or support staff).

- Staff/volunteers: report directly to the DSL (or deputy in their absence).
- Parents/carers: report to the headteacher or DSL.

Step 2 – DSL Action

The Designated Safeguarding Lead will:

- Log the concern in the school's online safety/safeguarding incident log.
- Assess the level of risk (low, medium, high) and determine next steps.
- Inform the headteacher of significant incidents.

Step 3 – Escalation

Depending on the seriousness of the incident, the DSL may escalate to:

- Headteacher – for behaviour/school management issues.
- Trust Director of Safeguarding – for advice, oversight, and if the incident has wider Trust implications.
- External agencies (e.g. local authority children's services, police, CEOP, Prevent duty team) where there is a risk of significant harm, criminal activity, or where possession/distribution of illegal material is suspected.

Step 4 – Governance Oversight

- The Local Governing Body will receive regular anonymised reports on online safety incidents, trends, and responses, at least termly.
- The Trust Board will be notified of serious incidents and will ensure appropriate lessons are learned.

Step 5 – Follow-up and Support

- Victims and, where appropriate, perpetrators will be offered pastoral and/or external support.
- Parents/carers will be informed where appropriate, unless this would place a child at further risk of harm.

All incidents will be reviewed to inform staff training, curriculum content, and the effectiveness of filtering/monitoring systems.

12. 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, 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 deputy 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.

Trust Directors and Local 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.

13. Monitoring arrangements

The DSL logs behaviour and safeguarding issues related to online safety. An incident report log can be found in the appendices.

This policy will be reviewed every year by the Director of Safeguarding. At every review, the policy will be renewed and approved by the Trust Board. The review will be supported by an annual risk assessment 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.

Links with other policies

This online safety policy is linked to our:

Child protection and safeguarding policy
Behaviour policy
Staff code of conduct
Staff disciplinary procedures
Data protection policy and privacy notices
Complaints procedure
IT and internet acceptable use policy

Appendix 2: Template 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 which 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: Template 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 which could harm the school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the school's network • Share my password with others or log in to the school's network using someone else's details • Take photographs of pupils without checking with teachers first • Share confidential information about the school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the school	
I will only use the school's 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 which might upset, distress or harm them or others, and will also do so if I encounter any such material. I will always use the school's IT systems and internet responsibly, and ensure that pupils in my care do so too.	
Signed (staff member/governor/volunteer/visitor):	**Date:**

Appendix 4: Template 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: Template 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**