The Charter School North Dulwich

ONLINE SAFETY POLICY

Author:	Head of Compliance	Date:	20 July 2026
Version:	2		
Reviewed by:	Trust Safeguarding Group	Date:	July 2026
Approved by:	Trust CEO	Date:	July 2026
Next Review Date:	July 2027		

Contents

1. Statement of Intent 2
2. Legislation and guidance 3
3. Roles and responsibilities 3
4. Educating pupils about online safety 8
5. Educating parents/carers about online safety 10
6. Cyber-bullying 11
7. Acceptable use of the internet in school 13
8. Pupils using mobile devices in school 14
9. Staff using work devices outside school 14
10. How the school will respond to issues of misuse 14
11. Training 15
12. Monitoring arrangements 16
13. Links with other policies 16

1. Statement of Intent

The Charter Schools Educational Trust (the 'Trust') understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the Trust's schools and therefore, there are a number of controls in place to ensure the safety of pupils and staff.

Our Trust and its schools aim to:

- Have robust processes in place to ensure the online safety of pupils, staff, supply staff, trainee teachers, contractors, volunteers and trustees 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' but can include smart watches, tablets and handheld games consoles)
- 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, extreme sexual or physical violence, misinformation, disinformation (including fake news) and conspiracy theories
- **Contact** – being subjected to harmful online interaction with other users or generative AI applications that simulate this; 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, including those generated using AI and online bullying, and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and or financial scams. If schools feel their pupils, students or staff are at risk, it should be reported to the Anti-Phishing Working Group (https://apwg.org/).

2. Legislation and guidance

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

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

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

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

This policy complies with our funding agreement and the articles of association.

3. Roles and responsibilities

3.1 The Trust Board and Local Governors

The Trust Board is ultimately responsible for safeguarding in the Trust's schools but the day-to-day strategic oversight of safeguarding standards, including online safety within each individual school, is delegated to the Local Governing Body (LGB), each of which will appoint a link governor responsible for safeguarding including online safety, and will ensure that their school complies with

their statutory duties and ensure that the policies, procedures and training in the schools are effective and comply with the law.

Trustees and local governors will receive appropriate training on safeguarding at induction that is updated regularly. In addition, they will receive information (for example, via emails, e-bulletins and newsletters) on safeguarding including online safety at least annually so that they can demonstrate knowledge of their responsibilities relating to the protection of children, young people and vulnerable adults.

The Trust Board will:

- Ensure that this policy is reviewed on an annual basis.
- Ensure their own knowledge of online safety issues is up to date.
- Ensure all staff undergo safeguarding and child protection training, including online safety, at induction and thereafter on an annual basis
- Ensure that there are appropriate filtering and monitoring systems in place in each of its schools and that the effectiveness of filtering and monitoring systems will be formally reviewed at least once every academic year.
- Ensure that all relevant Trust policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The Local Governing Body in each school is responsible for:

- Ensuring that that their school incorporates the principles of online safety across all elements of school life.
- Ensuring that the principles of online safety are reflected in the school's policies and practice where appropriate and that they are communicated with staff, pupils and parents.
- Via the link governor for safeguarding ensure that the school has appropriate filtering and monitoring systems in place on school devices and school networks and regularly review their effectiveness.
- Via the safeguarding link governor ensure the school is meeting the DFE Filtering and Monitoring standards, including:
    - 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 the school's safeguarding needs

All trustees and governors will:

- Make sure they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (Acceptable use policy)
- Make sure that online safety is a running and interrelated theme when devising and implementing the whole-trust approach to safeguarding and related policies and/or procedures

- Receive assurance regarding the effectiveness of filtering and monitoring systems and the outcomes of annual reviews.

3.2 The Trust Executive team

The Trust executive team including the CEO, Head of Compliance and Directors of Education are responsible for:

- ensuring that this policy is effective and complies with relevant laws and statutory guidance
- Updating the policy in line with any changes to statutory guidance or law and sharing across the Trust
- Ensuring schools are implementing the policy including reporting, recording, staff training and curriculum content

3.3 The Headteacher

The Headteacher (read also Principal) is responsible for making sure that all school staff understand this policy, and that it is being implemented consistently throughout the school. They are also responsible for:

- Designating a member of the senior leadership team to take strategic responsibility for filtering and monitoring arrangements.
- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the Designated Safeguarding Lead (DSL) and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL and ICT technicians to conduct termly light-touch reviews of this policy.
- Making sure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.4 The designated safeguarding lead (DSL)

Details of the school's designated safeguarding lead (DSL) and deputies (DDSLs) 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 making sure that staff understand this policy and that it is being implemented consistently throughout the school
- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking additional training as required so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND or vulnerable children face online.
- Working with the headteacher and the Trust Safeguarding Team to review this policy annually and make sure 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
- Providing governors with assurance that filtering and monitoring systems are working effectively and reviewed regularly
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the school's child protection policy
- Responding to safeguarding concerns identified by filtering and monitoring
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
- Ensuring all members of the school community understand the reporting procedure.

› Making sure that any online safety incidents or concerns are logged on CPOMs and dealt with appropriately in line with this policy as well as the actions taken in response to concerns

- Monitoring online safety incidents to identify trends and any gaps in the school's provision and using this data to update the school's procedures.
- Making sure 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 at least annually
- Liaising with other agencies and/or external services if necessary
- Reporting to the LGB about online safety on an annual basis as a minimum as part of the annual Safeguarding report, but more frequently should serious incidents or concerns arise.
- Undertaking annual risk assessments that consider and reflect the risks pupils 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.

3.5 The Trust Head of IT

The Trust Head of IT, working with the IT managed service provider, is responsible for:

- Ensuring that 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 make sure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Making sure 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 half-termly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files, including any reported suspicious emails
- Making sure that any online safety incidents they become aware of are reported to the school DSL
- Making sure that any incidents of cyber-bullying they become aware of are reported to the school DSL
- Ensuring that records will be maintained of filtering tests, monitoring reviews, identified issues and remedial actions taken.

This list is not intended to be exhaustive.

3.6 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 policy on acceptable use of the school's ICT systems and the internet, and making sure that pupils follow the school's terms on acceptable use
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing by contacting the DSL and IT Lead.
- Following the correct procedures by speaking to the DSL and IT Lead if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to make sure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Making sure that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

- Responding appropriately, in line with the Child Protection Policy and Procedures, to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'
- Ensuring they attend any required online safety training and have a good awareness of any current/common online safety issues.
- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Maintaining a professional level of conduct in their personal use of technology.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

This list is not intended to be exhaustive.

3.7 Parents/carers

Parents/carers are expected to:

- Notify a member of staff or the headteacher of any concerns or queries regarding this policy
- Make sure that their child has read, understood and agreed to the terms on acceptable use of the school's ICT 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
- Help and advice for parents/carers – Childnet
- Parents and carers resource sheet – Childnet

3.8 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy and expected to follow it. If appropriate, they will be expected to agree to the policy on acceptable use of technology.

4. Educating pupils about online safety

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

In line with the government's guidance on RSE and Health Education (From September 2026)

All schools have to teach:

- Relationships and sex education and health and wellbeing education

4.1 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

Pupils in **KS4** 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:

- Rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- Online risks, including the importance of being cautious about sharing personal information online and of using privacy and location settings appropriately to protect information online. Pupils should also understand the difference between public and private online spaces and related safety issues
- The characteristics of social media, including that some social media accounts are fake, and / or may post things which aren't real / have been created with AI. That social media users may say things in more extreme ways than they might in face-to-face situations, and that some users present highly exaggerated or idealised profiles of themselves online
- Not to provide material to others that they would not want to be distributed further and not to pass on personal material which is sent to them. Pupils should understand that any material provided online might be circulated, and that once this has happened there is no way of controlling where it ends up. Pupils should understand the serious risks of sending material to others, including the law concerning the sharing of images
- That keeping or forwarding indecent or sexual images of someone under 18 is a crime, even if the photo is of themselves or of someone who has consented, and even if the image was created by the child and/or using AI-generated imagery. Pupils should understand the potentially serious consequences of acquiring or generating indecent or sexual images of someone under 18, including the potential for criminal charges and severe penalties including imprisonment. Pupils should know how to seek support and should understand that they will not be in trouble for asking for help, either at school or with the police, if an image of themselves has been shared. Pupils should also understand that sharing indecent images of people over 18 without consent is a crime
- What to do and how to report when they are concerned about material that has been circulated, including personal information, images or videos, and how to manage issues online
- About the prevalence of deepfakes including videos and photos, how deepfakes can be used maliciously as well as for entertainment, the harms that can be caused by deepfakes and how to identify them
- That the internet contains inappropriate and upsetting content, some of which is illegal, including unacceptable content that encourages misogyny, violence or use of weapons. Pupils should be taught where to go for advice and support about something they have seen

online. Pupils should understand that online content can present a distorted picture of the world and normalise or glamorise behaviours which are unhealthy and wrong
- That social media can lead to escalations in conflicts, how to avoid these escalations and where to go for help and advice
- How to identify when technology and social media is used as part of bullying, harassment, stalking, coercive and controlling behaviour, and other forms of abusive and/or illegal behaviour and how to seek support about concerns
- That pornography, and other online content, often presents a distorted picture of people and their sexual behaviours and can negatively affect how people behave towards sexual partners. This can affect pupils who see pornographic content accidentally as well as those who see it deliberately. Pornography can also portray misogynistic behaviours and attitudes which can negatively influence those who see it
- How information and data is generated, collected, shared and used online
- That websites may share personal data about their users, and information collected on their internet use, for commercial purposes (e.g. to enable targeted advertising)
- That criminals can operate online scams, for example using fake websites or emails to extort money or valuable personal information. This information can be used to the detriment of the person or wider society. About risks of sextortion, how to identify online scams relating to sex, and how to seek support if they have been scammed or involved in sextortion
- That AI chatbots are an example of how AI is rapidly developing, and that these can pose risks by creating fake intimacy or offering harmful advice. It is important to be able to critically think about new types of technology as they appear online and how they might pose a risk

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.

4.2 Pupils will be taught practical cyber security skills

All pupils will receive age-appropriate training on safe internet use, including:

- Methods that hackers use to trick people into disclosing personal information
- Password security
- Social engineering
- The risks of removable storage devices (e.g. USBs)
- Multi-factor authentication
- How to report a cyber incident or attack
- How to report a personal data breach

Pupils will also receive age-appropriate education on safeguarding issues such as cyberbullying and the risks of online radicalisation.

5. Educating parents/carers about online safety

The school will raise parents/carers' awareness of online safety in letters or other communications home, and in information via the school website or other communication platforms as appropriate. This policy will also be shared with parents/carers.

The Trust will regularly update parents/carers as to the latest threats or concerns around online safety via the termly Trust Safeguarding magazine which will be distributed by its schools.

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 the school's Headteacher or the Trust Head of Compliance.

6. Cyber-bullying

6.1 Definition

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

6.2 Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and encourage them 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. Teachers will discuss cyber-bullying with their classes/tutor groups as appropriate

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 policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

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

6.3 Examining electronic devices

The headteacher, and any member of staff authorised to do so by the headteacher, can carry out a search and confiscate any 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 DSL
- Explain to the pupil why they are being searched, and 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 DSL 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 whether 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
- Our Positive Behaviour Policy

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

6.4 Artificial intelligence (AI)

Generative AI tools are now widespread and easy to access. Staff, pupils and parents/carers may be familiar with generative chatbots such as ChatGPT, Microsoft Copilot and Google Gemini.

The Charter Schools Educational Trust and its schools recognise that AI has many uses to help pupils learn but may also have the potential to be used to bully others. The Trust and its schools recognise that child-on-child abuse may involve AI-generated or digitally manipulated imagery and will respond to such incidents in line with safeguarding and child protection procedures. AI-related safeguarding risks may include deepfakes, nudification tools, AI-generated intimate images, AI-assisted bullying, impersonation, grooming, misinformation and inappropriate interactions with generative AI systems.

The Charter School North Dulwich will treat any use of AI to bully pupils very seriously, in line with our Positive Behaviour Policy, Child Protection and Safeguarding Policy and the Trust's Child on Child Abuse (including harmful sexual behaviour) Policy.

Staff should be aware of the risks of using AI tools while they are still being developed and should carry out a risk assessment where new AI tools are being used by the school in line with the Trust's AI Policy, and where existing AI tools are used in cases which may pose a risk to all individuals that may be affected by them, including, but not limited to, pupils and staff.

Any use of artificial intelligence should be carried out in accordance with our AI policy.

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 ICT 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.

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.

8. Pupils using mobile devices in school

Pupils may bring mobile devices into school, but these should be locked in their phone pouch and not seen or heard at any time during the school day, including:

- Lessons
- Tutor group time
- Social 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 (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.

9. Staff using work devices outside school

All staff members will take appropriate steps to ensure their work provided devices remain secure, working with their IT teams. This includes, but is not limited to:

- Keeping the device password-protected – strong passwords can be made up of 3 random words, in combination with numbers and special characters if required, or generated by a password manager
- 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 with any family or friends
- Ensuring that anti-virus and anti-spyware software is uploaded and updated regularly on the device
- Keeping operating systems up to date by promptly installing the latest updates

Staff members must not use the device in any way that would violate the Trust's terms of acceptable use.

Work devices must be used solely for work activities.

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

10. 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 including the school behaviour policy, our acceptable use policy and Child Protection Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

Where a staff member misuses the school's IT systems or the internet or misuses a personal device where the action constitutes misconduct, is in breach of the staff code of conduct or acceptable use policy the matter will be dealt with in accordance with the Trust Disciplinary Policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school, in consultation with relevant external agencies where appropriate, will consider whether incidents that involve serious online incidents, will be reported to the police.

11. Training

11.1 Staff, trustees, governors and volunteers

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. Staff training will also include awareness of AI-related safeguarding risks, including deepfakes, AI-generated imagery, nudification tools, AI-assisted bullying and misinformation.

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
  - Images can include any generated by AI that are used in the above scenarios.
- 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 DDSLs will undertake specific DSL 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.

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

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring arrangements

This policy will be reviewed every year by the Trust Head of Compliance. At every review the policy will be shared with the Trust and school leadership teams and the school's managed service provider.

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.

The effectiveness of filtering and monitoring systems will be formally reviewed at least once every academic year by the senior leader responsible for filtering and monitoring, with support from the school DSL and IT lead. Records of these reviews will be retained and reported to governors.

13. 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 policy and procedure
- ICT and internet acceptable use policies (pupils and staff)
- AI Policy