Online Safety Policy

Document Name	Online Safety Policy
Document written by	Miss K Jones
Date for next revision*	September 2027
Responsibility	St Barnabas
Date	September 2026

*subject to any relevant changes in legislation or other appropriate guidelines

Contents:

Statement of intent

1. Legal framework
2. Roles and responsibilities
3. Managing online safety
4. Cyberbullying
5. Child-on-child sexual abuse and harassment
6. Grooming and exploitation
7. Mental health
8. Online hoaxes and harmful online challenges
9. Cyber-crime
10. Online safety training for staff
11. Online safety and the curriculum
12. Use of technology in the classroom
13. Use of smart technology
14. Educating parents
15. Internet access
16. Filtering and monitoring online activity
17. Network security
18. Emails
19. Social networking
20. The school website
21. Use of devices
22. Generative AI and emerging technologies
23. Cyber security and information security
24. Filtering and monitoring assurance
25. Remote learning
26. Monitoring and review
27. Appendix A: Online risk areas and curriculum coverage
28. Appendix B: Key statutory guidance and supporting resources

Statement of intent

St Barnabas C of E Primary Academy 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 school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable, but they can be categorised into four areas of risk:

- **Content**: Being exposed to illegal, inappropriate or harmful material, e.g. pornography, fake news, self-harm and suicide, and discriminatory or extremist views.
- **Contact**: Being subjected to harmful online interaction with other users, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children.
- **Conduct**: Personal online behaviour that increases the likelihood of, or causes, harm, e.g. sending and receiving explicit messages, and cyberbullying.
- **Commerce**: Risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

The measures implemented to protect pupils and staff revolve around these areas of risk. Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

1. Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Keeping children safe in education 2026 (DfE) – statutory safeguarding guidance, in force from 1 September 2026.
- Working together to safeguard children 2026 – statutory guidance on multi-agency safeguarding arrangements.
- Relationships Education, Relationships and Sex Education (RSE) and Health Education – statutory guidance in force from 1 September 2026.
- Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR), as amended by the Data (Use and Access) Act 2025 where applicable.
- DfE, Meeting digital and technology standards in schools and colleges – including the Filtering and Monitoring: core standard and Cyber Security: core standard (updated September 2026).
- DfE, Teaching online safety in schools (updated January 2023).
- DfE, Searching, screening and confiscation in schools (updated July 2023).
- UK Council for Internet Safety, Sharing nudes and semi-nudes: advice for education settings working with children and young people (updated March 2024).
- UK Council for Internet Safety, Education for a Connected World – 2020 edition.
- Prevent duty guidance: England and Wales (2023), together with current DfE practical guidance for designated safeguarding leads.
- DfE, Data protection in schools (updated July 2026), including guidance on filtering and

monitoring, photographs and videos, and generative AI and data protection.

This policy operates in conjunction with the following school policies:

- Safeguarding and Child Protection Policy
- Anti bullying Policy
- Relationships and Health Education Policy
- Positive behaviour and self-esteem policy
- Technology Acceptable Use Agreement

1.1 Roles and responsibilities

The local advisory board is responsible for:

- ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- ensuring the Designated Safeguarding Leads remit covers online safety.
- reviewing this policy on an annual basis.
- ensuring their own knowledge of online safety issues is up-to-date.
- ensuring all staff undergo safeguarding and child protection training, including online safety, at induction.
- ensuring that there are appropriate filtering and monitoring systems in place.
- ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The Executive Headteacher is responsible for:

- 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 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 local advisory board to update this policy on an annual basis.
- reporting to the local advisory board about online safety on a termly basis.

The Designated Safeguarding Lead is responsible for:

- taking the lead responsibility for online safety in the school.
- acting as the named point of contact within the school on all online safeguarding issues.

- undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians.
- ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- ensuring safeguarding is considered in the school's approach to remote learning.
- ensuring appropriate referrals are made to external agencies, as required.
- working closely with the police during police investigations.
- keeping up-to-date with current research, legislation and online trends.
- coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- 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.
- maintaining records of reported online safety concerns 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.
- working with the Executive Headteacher and governing board to update this policy on an annual basis.

Trust IT Team/Securely are responsible for:

- providing technical support in the development and implementation of the school's online safety policies and procedures.
- implementing appropriate security measures as directed by the Executive Headteacher.
- ensuring that the school's filtering and monitoring systems are updated as appropriate.

All staff members are responsible for:

- taking responsibility for the security of ICT systems and electronic data they use or have access to.
- modelling good online behaviours.
- maintaining a professional level of conduct in their personal use of technology.
- having an awareness of online safety issues.
- ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- reporting concerns in line with the school's reporting procedure.
- where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils are responsible for:

- adhering to the Acceptable Use Agreement and other relevant policies.
- seeking help from school staff if they are concerned about something they or a peer have experienced online.

- reporting online safety incidents and concerns in line with the procedures within this policy.

2. Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people, particularly owing to the rise of social media and the increased prevalence of children using the internet.

The DSL has overall responsibility for the school's approach to online safety, with support from deputies and the Executive Headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

- Staff and governors receive regular safeguarding training
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum
- Regular online safety newsletters are shared with parents, pupils and staff
- Dedicated pages for parents and pupils linked to online safety are on the school website

Handling online safety concerns

Online safety concerns are safeguarding concerns. All staff must act promptly, maintain a child-centred approach and follow the school's Safeguarding and Child Protection Policy. Staff must not promise confidentiality and must record and report concerns without delay.

Do not investigate beyond what is necessary to establish immediate safety; avoid leading questions and do not ask a child to repeat information unnecessarily.

Where a concern indicates that a child is at risk of significant harm, an immediate referral will be made to children's social care and/or the police in accordance with safeguarding procedures.

Information will be shared lawfully and on a need-to-know basis, with the child's welfare as the paramount consideration.

Online safeguarding incidents will be recorded accurately on CPOMS or the school's designated safeguarding recording system, including actions and outcomes.

Any disclosures made by pupils to staff members about online abuse, harassment or exploitation, whether they are the victim or disclosing on behalf of another child, will be handled in line with the Safeguarding and Child Protection Policy.

Staff will be aware that pupils may not feel ready or know how to tell someone about abuse they are experiencing, due to feeling embarrassed, humiliated, or threatened. Staff will be aware and

recognise the importance of the presence and scale of online abuse or harassment, by considering that just because it is not being reported, does not mean it is not happening.

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The Safeguarding and Child protection policy linked to disclosure will be followed. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully and appropriate support provided to the victim.

Concerns regarding a staff member's online behaviour are reported to the Executive Headteacher, who decides on the best course of action in line with Low level concerns with the Safeguarding and Child Protection Policy and further relevant policies, e.g. St Barnabas Staff Induction handbook; Vantage Academy Trust handbook; ICT acceptable use agreement. If the concern is about the Executive Headteacher, it is reported to the chair of governors.

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the Executive Headteacher and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Safeguarding and Child Protection Policy.

Where there is a concern that illegal activity has taken place, the Executive Headteacher contacts the police.

The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and as a result of ignorance or normal developmental curiosity, e.g. a pupil has taken and distributed indecent imagery of themselves. The DSL will decide in which cases this response is appropriate and will manage such cases in line with the Safeguarding and Child Protection Policy.

All online safety incidents identified by staff or through securely are recorded on CPOMS and the school's response are recorded by the DSL.

3. Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- threatening, intimidating or upsetting text messages
- threatening or embarrassing pictures and video clips sent via mobile phone cameras
- silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- unpleasant messages sent via instant messaging

- unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- abuse between young people in intimate relationships online i.e. teenage relationship abuse
- discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the Anti-bullying Policy.

4. Child-on-child sexual abuse and harassment

Pupils may also use the internet and technology as a vehicle for sexual abuse and harassment. Staff will understand that this abuse can occur both in and outside of school, off and online, and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

The following are examples of online harmful sexual behaviour of which staff will be expected to be aware:

- threatening, facilitating or encouraging sexual violence
- upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- sexualised online bullying, e.g. sexual jokes or taunts
- unwanted and unsolicited sexual comments and messages
- consensual or non-consensual sharing of sexualised imagery
- abuse between young people in intimate relationships online, i.e. teenage relationship abuse

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

Staff will be aware that creating, possessing, and distributing indecent imagery of other children, i.e. individuals under the age of 18, is a criminal offence, even where the imagery is created, possessed, and distributed with the permission of the child depicted, or by the child themselves.

The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking "sides", often leading to repeat harassment. The school will respond to these incidents in line with the Safeguarding and Child Protection Policy.

The school responds to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned

equipment. Concerns regarding online child-on-child abuse are reported to the DSL, who will investigate the matter in line with the Safeguarding and Child Protection Policy.

Sharing nudes and semi-nudes: any incident involving nude or semi-nude images, videos or live streams of a person under 18 will be treated as a safeguarding concern and referred to the DSL immediately. Staff must never view, copy, print, forward, save or store such imagery, or ask a child to send or download it. If imagery is shown accidentally, the member of staff must stop viewing it, report immediately to the DSL and follow safeguarding procedures.

- The DSL will follow the current UKCIS guidance, including consideration of whether the incident involves coercion, exploitation, an adult, wider safeguarding concerns or immediate risk of harm.
- If an adult is involved in the production or sharing of sexual imagery involving a child, the concern will be treated as child sexual abuse and referred to the police and children's social care as appropriate.
- The school will avoid victim-blaming or shaming and will provide appropriate support to all children involved, while managing harmful sexual behaviour in accordance with the Safeguarding and Child Protection and Behaviour Policies.

5. Grooming and exploitation

Grooming is defined as the situation whereby an adult builds a relationship, trust and emotional connection with a child with the intention of manipulating, exploiting and/or abusing them.

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, including the following:

- the pupil believes they are talking to another child, when they are actually talking to an adult masquerading as someone younger with the intention of gaining their trust to abuse them.
- the pupil does not want to admit to talking to someone they met on the internet for fear of judgement, feeling embarrassed, or a lack of understanding from their peers or adults in their life.
- the pupil may have been manipulated into feeling a sense of dependency on their groomer due to the groomer's attempts to isolate them from friends and family.
- talking to someone secretly over the internet may make the pupil feel 'special', particularly if the person they are talking to is older.
- the pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and

what the signs of online grooming are, including:

- being secretive about how they are spending their time.
- having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

Child sexual exploitation (CSE) and child criminal exploitation (CCE)

Although CSE often involves physical sexual abuse or violence, online elements may be prevalent, e.g. sexual coercion and encouraging children to behave in sexually inappropriate ways through the internet. In some cases, a pupil may be groomed online to become involved in a wider network of exploitation, e.g. the production of child pornography or forced child prostitution and sexual trafficking.

CCE is a form of exploitation in which children are forced or manipulated into committing crimes for the benefit of their abuser, e.g. drug transporting, shoplifting and serious violence. While these crimes often take place in person, it is increasingly common for children to be groomed and manipulated into participating through the internet.

Where staff have any concerns about pupils with relation to CSE or CCE, they will bring these concerns to the DSL without delay, who will manage the situation in line with the Safeguarding and Child Protection Policy.

Radicalisation

Radicalisation is the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. This process can occur through direct recruitment, e.g. individuals in extremist groups identifying, targeting and contacting young people with the intention of involving them in terrorist activity, or by exposure to violent ideological propaganda. Children who are targets for radicalisation are likely to be groomed by extremists online to the extent that they believe the extremist has their best interests at heart, making them more likely to adopt the same radical ideology.

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the school's Prevent Duty. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Prevent Duty.

6. Mental Health

The internet, particularly social media, can be the root cause of a number of mental health issues in pupils, e.g. low self-esteem and suicidal ideation.

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will undergo mental health first aid training which will be disseminated to staff to ensure staff members understand popular social media sites and terminology, the ways in which social media and

the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be reported to the DSL via CPOMS concerns.

7. Online hoaxes and harmful online challenges

For the purposes of this policy, an **"online hoax"** is defined as a deliberate lie designed to seem truthful, normally one that is intended to scaremonger or to distress individuals who come across it, spread on online social media platforms.

For the purposes of this policy, **"harmful online challenges"** refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.

The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the Executive Headteacher will decide whether each proposed response is:

- in line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- careful to avoid needlessly scaring or distressing pupils.
- not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- proportional to the actual or perceived risk.
- helpful to the pupils who are, or are perceived to be, at risk.
- appropriate for the relevant pupils' age and developmental stage.
- supportive.
- in line with the Safeguarding and Child Protection Policy.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, e.g. it encourages children to participate in age-inappropriate activities that could increase safeguarding risks or become a child protection concern, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly

affected or even to individual children at risk where appropriate. The Executive Headteacher will liaise directly with children's social care for advice.

The DSL and Executive Headteacher will only implement a school-wide approach to highlighting potential harms of a hoax or challenge when the risk of needlessly increasing pupils' exposure to the risk is considered and mitigated as far as possible.

8. Cyber-crime

Cyber-crime is criminal activity committed using computers and/or the internet. There are two key categories of cyber-crime:

- **Cyber-enabled** – these crimes can be carried out offline; however, are made easier and can be conducted at higher scales and speeds online, e.g. fraud, purchasing and selling of illegal drugs, and sexual abuse and exploitation.
- **Cyber-dependent** – these crimes can only be carried out online or by using a computer, e.g. making, supplying or obtaining malware, illegal hacking, and 'booting', which means overwhelming a network, computer or website with internet traffic to render it unavailable.

The school will factor into its approach to online safety the risk that pupils with a particular affinity or skill in technology may become involved, whether deliberately or inadvertently, in cyber-crime. Where there are any concerns about a pupil's use of technology and their intentions with regard to using their skill and affinity towards it, the DSL will consider a referral to the Cyber Choices programme, which aims to intervene where children are at risk of committing cyber-crime and divert them to a more positive use of their skills and interests.

The DSL and Executive Headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully, and will ensure that pupils cannot access sites or areas of the internet that may encourage them to stray from lawful use of technology, e.g. the 'dark web', on school-owned devices or on school networks through the use of appropriate firewalls.

9. Online safety training for staff

The DSL ensures that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

Information about the school's full responses to online safeguarding incidents can be found in the Anti-bullying Policy and the Safeguarding and Child Protection Policy.

10. Online safety and the curriculum

Online safety is embedded throughout the curriculum; however, it is particularly addressed

in the following subjects:

- Jigsaw (PSHE inc Relationships and Health Education)
- Computing (Purple Mash scheme has online safety unit in each year group)
- Internet Safety Day
- Within research in International Primary Curriculum

Online safety teaching is always appropriate to pupils' ages and developmental stages.

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- how to evaluate what they see online
- how to recognise techniques used for persuasion
- what healthy and respectful relationships, including friendships, look like
- body confidence and self-esteem
- consent, e.g. with relation to the sharing of indecent imagery or online coercion to perform sexual acts
- acceptable and unacceptable online behaviour
- how to identify online risks
- how and when to seek support
- how to identify when something is deliberately deceitful or harmful
- how to recognise when something they are being asked to do puts them at risk or is age-inappropriate

The online risks pupils may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in appendix A of this policy.

Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and children looked after. Relevant members of staff, e.g. the SENCO and designated teacher for children looked after, work together to ensure the curriculum is tailored so these pupils receive the information and support they need.

The school will also endeavour to take a more personalised or contextualised approach to teaching about online safety for more susceptible children, and in response to instances of harmful online behaviour from pupils.

Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils. When reviewing these resources, the following questions are asked:

- Where does this organisation get their information from?
- What is their evidence base?

- Have they been externally quality assured?

- What is their background?
- Are they age-appropriate for pupils?
- Are they appropriate for pupils' developmental stage?

Before conducting a lesson or activity on online safety, the class teacher and DSL consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL advises the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities are planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher ensures a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Safeguarding and Child Protection Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Safeguarding and Child Protection Policy.

Generative AI and emerging technologies

- The school recognises that generative AI and other emerging technologies can create benefits and risks for teaching, learning and safeguarding. Any use must be planned, age-appropriate, proportionate and consistent with the school's safeguarding, data protection, acceptable use and curriculum arrangements.
- Pupils will only use pupil-facing generative AI tools where the school has assessed the tool as suitable for the age group and has appropriate safeguards, including supervision, filtering and monitoring, privacy and data protection arrangements.
- Staff will not enter confidential, sensitive or personal information about pupils, families or colleagues into generative AI tools unless the tool and proposed processing have been approved through the school's data protection and information governance arrangements.
- The school will comply with age restrictions and the safety requirements of AI products. Staff and pupils will be taught to recognise inaccurate, biased, manipulative or harmful AI-generated content, including deepfakes and impersonation.
- Where AI is used to support teaching, assessment or administration, a member of staff remains responsible for checking accuracy, appropriateness, safeguarding implications and copyright/data protection requirements before content is used.
- The DSL, Executive Headteacher and digital/IT lead will consider AI-related safeguarding risks when reviewing filtering, monitoring, acceptable use, staff training and curriculum provision.

11. Use of technology in the classroom

A wide range of technology is used during lessons, including the following:

- Computers
- Chromebooks
- Tablets
- Google Classroom
- Cameras

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher always reviews and evaluates the resource. Class teachers ensure that any internet-derived materials are used in line with copyright law.

Pupils are supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

12. Use of smart technology

While the school recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages.

Pupils will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the school's Technology Acceptable Use Agreement for Pupils.

Staff will use all smart technology and personal technology in line with the Trust ICT acceptable user agreement.

Pupils will not be permitted to use personal smart devices such as mobile phones. These devices will be handed into to school office and collected at the end of the school day by older pupils within school.

Staff are not permitted to use personal smart devices in school during working hours. Staff will ensure these are not visible to pupils and will only be used during lunch breaks.

13. Educating parents

The school works in partnership with parents to ensure pupils stay safe online at school and at home. Parents are provided with information about the school's approach to online safety and their role in protecting their children. This is detailed on the school website and shared through regular tweets from the National Online Safety website.

Parents will be made aware of the various ways in which their children may be at risk online, and encouraged to converse with their children linked to their online behaviour.

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.

Parental awareness regarding how they can support their children to be safe online is raised in

the following ways:

- Parents' evenings
- School Website
- School X (Twitter) account
- Newsletters
- Online resources
- Conversations with the learning mentor

14. Internet access

Pupils, staff and other members of the school community are only granted access to the school's internet network once they have read and signed the Acceptable Use Agreement. A record is kept of users who have been granted internet access in the school office.

All members of the school community are encouraged to use the school's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

15. Filtering and monitoring online activity

The local advisory board / Executive Headteacher ensures the school's ICT network has appropriate filters and monitoring systems in place. The local advisory board / Executive Headteacher ensures 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The filtering and monitoring systems the school implements are appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks.

Requests regarding making changes to the filtering system are directed to the Executive Headteacher. Prior to making any changes to the filtering system, ICT technicians and the DSL conduct a risk assessment. Any changes made to the system are recorded by Trust IT Team. Reports of inappropriate websites or materials are made to the Executive Headteacher / DSL immediately, who investigates the matter and makes any necessary changes.

Deliberate breaches of the filtering system are reported to the DSL and ICT technicians, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Positive Behaviour and Self Esteem Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.

The school's network and school-owned devices are appropriately monitored via Securely. All users of the network and school-owned devices are informed about how and why they are monitored through annual safeguarding training. Concerns identified through monitoring

are reported to the DSL who manages the situation in line with the Safeguarding and Child Protection Policy.

Filtering and monitoring assurance

- Filtering and monitoring will be reviewed and tested regularly to confirm that they are effective, proportionate and appropriate for the age and needs of pupils, including pupils with SEND.
- The DSL, Executive Headteacher and IT support will work together to understand the purpose, scope and operation of filtering and monitoring, including what alerts are generated, who receives them and how concerns are escalated.
- The school will maintain evidence of filtering and monitoring checks, actions and reviews and will address identified weaknesses promptly.
- Filtering will not be relied upon as the sole safeguarding measure. Staff supervision, curriculum education, acceptable use expectations, reporting routes and professional judgement remain essential.
- The school will consider AI-generated content and new technologies when assessing filtering and monitoring arrangements.

Cyber security and information security

- The school will maintain proportionate cyber security arrangements to protect pupils, staff, systems and personal data and to reduce safeguarding risks arising from loss of access, unauthorised access, malware or data breaches.
- A cyber risk assessment will be completed at least annually and reviewed each term, and additionally following significant technology or process changes or a cyber incident.
- The school and its IT support provider will maintain appropriate security updates, anti-malware and firewall protection, secure user accounts and access controls, reliable backups and recovery arrangements, and appropriate incident reporting arrangements.
- Staff will receive regular cyber security awareness training, including phishing, social engineering, password security, device security, reporting of incidents and protection of personal information.
- Any suspected cyber attack, significant security weakness or personal data breach will be reported promptly through the school's established IT, safeguarding and data protection procedures.

16. Network security

Technical security features, such as anti-virus software, are kept up-to-date and managed by Trust IT Team. Firewalls are switched on at all times. Trust IT Team technicians review the firewalls regularly to ensure they are running correctly, and to carry out any required updates.

Staff and pupils are advised not to download unapproved software or open unfamiliar email attachments, and are expected to report all malware and virus attacks to Trust IT Team.

All members of staff have their own unique usernames and private passwords to access the school's systems. Pupils are provided with their own unique username and private passwords. Staff members and pupils are responsible for keeping their passwords private. Passwords have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible. Passwords expire and users are required to change them.

Users inform Trust IT Team if they forget their login details, who will arrange for the user to reset their log in and passwords. Users are not permitted to share their login details with others and are not allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the Executive Headteacher is informed and decides the necessary action to take.

Users are required to lock access to devices and systems when they are not in use.

17. Emails

Staff are given approved school email accounts and are only able to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff must agree to and sign the Acceptable Use Agreement. Personal email accounts are not permitted to be used on the school site. Any email that contains sensitive or personal information is only sent using secure and encrypted email.

Staff members and pupils are required to block spam and junk mail, and report the matter to Trust IT Team. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils are made aware of this. Chain letters, spam and all other emails from unknown sources are deleted without being opened.

Any cyber-attacks initiated through emails are managed by Trust IT Team.

18. Social Networking Personal use

Access to social networking sites is filtered as appropriate. Staff and pupils are not permitted to use social media for personal use during lesson time/school day. Staff can use personal social media during break and lunchtimes; however, inappropriate or excessive use of personal social media during school hours may result in the removal of internet access or further action. Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school. The Staff Code of Conduct within the staff induction handbook contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.

Staff receive training on how to use social media safely and responsibly. Staff are not permitted to communicate with pupils or parents over social networking sites and are reminded to alter their privacy settings to ensure pupils and parents are not able to contact them on social media. Where staff have an existing personal relationship with a parent or pupil, and thus are

connected with them on social media, e.g. they are friends with a parent at the school, they will disclose this to the DSL and Executive Headteacher and will ensure that their social media conduct relating to that parent is appropriate for their position in the school.

Pupils are taught how to use social media safely and responsibly through the online safety curriculum. Parents are given advice linked to various social media platforms. Concerns regarding the online conduct of any member of the school community on social media are reported to the DSL and managed in accordance with the relevant policy.

Use on behalf of the school

The use of social media on behalf of the school is conducted in line with this policy. The school's official social media channels are only used for official educational or engagement purposes. The Assistant and Deputy principals are authorised by the Executive Headteacher to access to the school's social media accounts.

All communication on official social media channels on behalf of the school is clear, transparent and open to scrutiny.

19. The school website

The Executive Headteacher is responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law. Personal information relating to staff and pupils is not published on the website. Images and videos are only posted on the website if the permission is granted.

20. Use of devices School-owned devices

Staff members are issued with the following devices to assist with their work:

- Class Computer
- Laptop
- Tablet

Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g. tablets/chromebooks/laptops to use during lessons.

School-owned devices are used in accordance with the User Agreement. Staff and pupils are not permitted to connect school-owned devices to public Wi-Fi networks. All school-owned devices are password protected. Staff are expected to bring school devices into school on a weekly basis to ensure they are updated and synced.

Trust IT Team review all school-owned devices regularly to carry out software updates and ensure there is no inappropriate material or malware on the devices. No software, apps or other programmes can be downloaded onto a device without authorisation from Trust IT Team.

Cases of staff members or pupils found to be misusing school-owned devices will be managed

in line with the Positive Behaviour and Self Esteem Policy and Safeguarding and Child Protection Policy.

Personal devices

Any personal electronic device that is brought into school is the responsibility of the user. Pupils are expected to hand in any personal devices to the school office.

Personal devices are not permitted to be used in the following locations:

- Toilets
- Classrooms
- Shared areas

Staff members are not permitted to use their personal devices during lesson time, other than in an emergency which needs to be authorised by the Executive Headteacher. Staff members are not permitted to use their personal devices to take photos or videos of pupils or their learning.

Staff members report concerns about their colleagues' use of personal devices on the school premises in line with the Safeguarding and Child Protection Policy. If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the Executive Headteacher will seek advice from the Local Authority Designated Officer (LADO) and the police.

Pupils' devices can be searched, screened and confiscated in accordance with the Searching, Screening and Confiscation section of the Positive Behaviour and Self Esteem Policy. If a staff member reasonably believes a pupil's personal device has been used to commit an offence or may provide evidence relating to an offence, the device will be handed to the police. It will be turned off immediately and staff will not access anything on the pupils' personal device.

Appropriate signage is displayed to inform visitors to the school of the expected use of personal devices. Any concerns about visitors' use of personal devices on the school premises are reported to the DSL.

21. Remote learning

All remote learning is delivered in line with the school's Remote Learning Policy.

The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use. The school will consult with parents prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

During the period of remote learning, the school will maintain regular contact with parents to:

- reinforce the importance of children staying safe online.
- ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
- encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- direct parents to useful resources to help them keep their children safe online.

The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

Remote learning safeguarding arrangements

- Where remote learning is required, safeguarding expectations remain the same as when pupils are in school. Staff will use approved platforms and accounts and will maintain professional boundaries.
- Any online lesson, meeting or communication with pupils will be conducted through school-approved systems, with appropriate supervision and recording arrangements where required.
- Concerns arising during remote learning will be reported immediately to the DSL and managed under the Safeguarding and Child Protection Policy.
-

22. Monitoring and review

- The DSL, Executive Headteacher and IT support will monitor the effectiveness of this policy through safeguarding records, filtering and monitoring reports, staff feedback, curriculum review, incident analysis, training records and periodic technical assurance.
- The policy will be reviewed in full at least annually and sooner where there are significant changes to legislation, statutory guidance, technology, school systems or safeguarding risks.
- The Local Advisory Board will receive appropriate assurance that filtering and monitoring arrangements are in place, are understood by relevant staff and are reviewed for effectiveness.
- Lessons from incidents, near misses, complaints, pupil voice and parent feedback will be used to improve practice.

The school recognises that the online world is constantly changing; therefore, the DSL, Trust IT Team and the Executive Headteacher conduct termly light-touch reviews of this policy to evaluate its effectiveness.

The local advisory board, Executive Headteacher and DSL review this policy in full on an annual basis and following any online safety incidents.

The next scheduled review date for this policy is September 2027.
Any changes made to this policy are communicated to all members of the school community.

Appendix A: Online risk areas and curriculum coverage

The curriculum is reviewed against the four broad online risk areas of Content, Contact, Conduct and Commerce. Coverage is adapted to pupils' age, developmental stage, individual needs and current online experiences.

Content – illegal, inappropriate or harmful material; misinformation, disinformation and conspiracy theories; pornography; self-harm and suicide content; hate or discriminatory material; extremist content; harmful AI-generated or manipulated content.

Contact – grooming, exploitation, coercion, unwanted contact, abusive relationships, bullying, sexual harassment, pressure from peers, adults posing as children and harmful interactions in gaming or social platforms.

Conduct – cyberbullying, harmful sexual behaviour, sharing images without consent, unsafe posting, impersonation, digital footprints, privacy, passwords, scams, excessive or inappropriate use and behaviour that may cause harm to self or others.

Commerce – phishing, fraud, scams, in-app purchases, gambling-related content, targeted advertising, commercial pressure, financial exploitation and unsafe sharing of financial or personal information.

Pupils are taught how to evaluate online information, recognise persuasion and manipulation, use respectful communication, protect personal information, report concerns, seek trusted adult help and make safer choices.

Online safety education is embedded through Relationships Education, Health Education, Computing and other relevant curriculum areas. External resources are checked for accuracy, safeguarding, age-appropriateness, accessibility and developmental suitability before use.

Appendix B: Key statutory guidance and supporting resources

This policy should be read alongside the current versions of the following documents and resources. Where guidance is updated, the latest version should be followed.

Department for Education – Keeping children safe in education 2026.

Department for Education – Working together to safeguard children 2026.

Department for Education – Relationships Education, Relationships and Sex Education (RSE) and Health Education, effective from 1 September 2026.

Department for Education – Meeting digital and technology standards in schools and colleges: Filtering and monitoring and Cyber security core standards, updated September 2026.

Department for Education – Teaching online safety in schools.

Department for Education – Searching, screening and confiscation in schools.

UK Council for Internet Safety – Sharing nudes and semi-nudes: advice for education settings working with children and young people, updated March 2024.

Home Office – Prevent duty guidance: England and Wales (2023), and current DfE practical guidance for designated safeguarding leads.

Department for Education – Generative artificial intelligence (AI) in education; Generative AI: product safety standards; and related AI support materials for 2026–27.

Department for Education – Data protection in schools, updated July 2026.

National Cyber Security Centre – cyber security guidance for schools and education settings.

UK Council for Internet Safety – Education for a Connected World, 2020 edition.