

St. Bernadette's Catholic Primary School

Online Safety Policy

2026/2027



At St. Bernadette's Catholic Primary School, you will find us caring, hardworking and co-operative. We follow the ways of Jesus using our talents and gifts to make our school special. We show respect to all and welcome you.

Policy owner	Mrs Kidner
Named senior leader	Miss Finnegan
Signed by Headteacher	
Approved by	Governing Body
Approval date	October 2026
Signed by Chair of Governors	
Review date	September 2027, or sooner following an incident, near miss or change in guidance
Policy status	Statutory school policy
Publication	School website; available in hard copy on request

Statement of intent

Saint Bernadette's 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:** Exposure to illegal, inappropriate or harmful content, including pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation and conspiracy theories.
- **Contact:** Harmful online interaction with other users or generative AI applications that simulate this, including peer pressure, commercial advertising and adults posing as children or young adults to groom or exploit them sexually, criminally, financially or otherwise.
- **Conduct:** Online behaviour that increases the likelihood of, or causes, harm, including making, sending and receiving explicit images, including those generated using AI, and online bullying.
- **Commerce:** Risks including online gambling, inappropriate advertising, phishing and 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:

- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2026) Keeping Children Safe in Education
- DfE (2026) Filtering and Monitoring: core standard
- DfE (2021) Harmful online challenges and hoaxes
- DfE (2023) Teaching online safety in school
- DfE (2022) Searching, screening and confiscation
- DfE (2026) Generative AI: product safety standards
- DfE (2026) Mobile phones in schools
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2020) 'Small Business Guide: Cyber Security'

2. Roles and responsibilities

The governing board will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSLs 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 and at regular intervals.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.

The headteacher will be 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 DSLs 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.
- 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 DSLs and ICT Operations Manager to conduct termly light-touch reviews of this policy.
- Working with the DSLs and governing board to update this policy on an annual basis.

The DSLs will be responsible for:

- Alongside the Computing Lead, taking the lead responsibility for online safety in the school.
- 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 the ICT Operations Manager.
- 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 online safety incidents and inappropriate internet use is reported via MyConcern, and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- 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 headteacher and governing board to update this policy on an annual basis.

The ICT Operations Manager will be 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 headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

All staff members will be 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 will be 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.

3. 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 DSLs have overall responsibility for the school's approach to online safety, with support from the Computing Lead and the headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSLs 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 training
- Staff receive email updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum
- Online safety and safeguarding messages are reinforced regularly through the curriculum, assemblies and targeted teaching, including Safer Internet Day.
- Parents are invited to attend an online safety workshop in the week of Safer Internet Day
- Pupils access online content through school-managed devices and networks with appropriate filtering, monitoring and age-appropriate supervision.

Handling online safety concerns

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 Child Protection and Safeguarding Policy.

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 DSLs will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it

is necessary in order to protect them from further harm. Ultimately the DSLs will balance the victim's wishes against their duty to protect the victim and other young people. The DSLs 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, for example, if the DSLs decide that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. 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 – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

Concerns regarding a staff member's online behaviour are reported to the headteacher, who decides on the best course of action in line with the relevant policies. If the concern is about the headteacher, it is reported to the chair of governors.

Concerns regarding a pupil's online behaviour are reported to the DSLs, who investigate concerns with relevant staff members, e.g. the headteacher and ICT Operations Manager, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the school will consider whether a referral to the police or other appropriate agency is required, in consultation with the DSL and in line with the Child Protection and Safeguarding Policy.

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 Child Protection and Safeguarding Policy.

All online safety incidents and the school's response are recorded by the DSLs.

4. 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.

5. 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
- Sharing self-generated intimate images and/or videos, including images or videos generated or manipulated using artificial intelligence
- 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 self-generated intimate images and/or videos of children, including images or videos generated or manipulated using artificial intelligence, can constitute a criminal offence.

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 Child-on-child Abuse Policy.

The school will respond 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 will be reported to the DSLs, who will investigate the matter in line with the Child-on-child Abuse Policy and the Child Protection and Safeguarding Policy.

6. 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, e.g. 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 DSLs 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 online.
- 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 sexual abuse material or sexual exploitation or trafficking of children.

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 Child Protection and Safeguarding 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 Prevent Duty Policy. 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 DSLs without delay, who will handle the situation in line with the Prevent Duty Policy.

7. Mental health

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 DSLs will ensure that training is available to help ensure that 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 dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy.

8. 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 DSLs immediately.

The DSLs 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 DSLs 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 DSLs 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 Child Protection and Safeguarding Policy.

Where the DSLs assessment finds an online challenge to be putting pupils at risk of harm, 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 individual pupils at risk where appropriate.

The DSLs 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.

9. Online safety training for staff

The DSLs will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. 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.

10. Online safety and the curriculum

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

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
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- Knowledge and behaviours that are covered in the government's online media literacy strategy
- How artificial intelligence and AI-generated content can be used safely and responsibly, including understanding of the potential risks of AI-generated or manipulated content

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.

The DSLs will be involved with the development of the school's online safety curriculum. 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.

Relevant members of staff, e.g. the SENCO and designated teacher for LAC, will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and LAC, 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 will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum.

Before conducting a lesson or activity on online safety, the class teacher and DSLs will 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 DSLs will advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities will be 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 will ensure 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 Child Protection and Safeguarding 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 Child Protection and Safeguarding Policy.

II. Use of technology in the classroom

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

- Computers
- Laptops
- Tablets
- School Network
- Email
- 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 will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

Pupils will be 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 school's Computing Acceptable Use Policy.

Inappropriate use of smart technology may include:

- Using mobile and smart technology to sexually harass, bully, troll or intimidate peers.
- Sharing indecent images, both consensually and non-consensually.
- Viewing and sharing pornography and other harmful content.

St Bernadette's Catholic Primary School is a mobile-phone-free school. Pupils must not have access to, or use, mobile phones or personal smart devices with communication or recording functions during the school day, including lessons, transitions, breaktimes and lunchtimes.

We recognise that some older pupils who walk to or from school independently may need to carry a mobile phone for safety while travelling. Where a parent/carer considers this necessary, they must complete the school's Mobile Phone Request Form and receive agreement from the school before their child brings a phone onto the school site.

Where permission has been granted, the phone must be switched off before the pupil enters the school site and handed directly to Mr Carroll at the beginning of the school day. Phones will be stored securely in a locked drawer and will not be accessible to pupils during the school day. The phone will be returned at the end of the school day for the pupil's journey home. In Mr Carroll's absence, a nominated member of SLT will oversee collection, secure storage and return.

Permission to bring a phone to school does not give permission for the phone to be used during the school day. Pupils must not use personal devices to make calls, send messages, access social media or the internet, take photographs, make audio or video recordings or communicate with others while on the school premises or during school activities.

Where a pupil brings a phone to school without permission, fails to hand it in, or accesses or uses a device during the school day, the phone may be confiscated in accordance with the school's procedures and parents/carers will be informed. Any further response will be reasonable and proportionate and in line with the Behaviour Policy and Mobile Phone Policy.

Any exceptions to the school's mobile phone arrangements will be considered on an individual basis where required to meet the pupil's medical, SEND, safeguarding or other specific needs. Any such arrangements will be agreed with the school and managed appropriately.

Where there is a significant problem with the misuse of smart technology among pupils, the school will discipline those involved in line with the school's Behaviour Policy.

The school will hold assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

The Computing Lead will seek to ensure that it is kept up to date with the latest devices, platforms, apps, trends and related threats.

The school will consider the 4Cs (content, contact, conduct and commerce) when educating pupils about the risks involved with the inappropriate use of smart technology and enforcing the appropriate disciplinary measures.

13. Educating parents

The school will work in partnership with parents to ensure pupils stay safe online at school and at home. Parents will be provided with information about the school's approach to online safety and their role in protecting their children. Parents will be sent a copy of the Acceptable Use Agreement at the beginning of each academic year and are encouraged to go through this with their child to ensure their child understands the document and the implications of not following it.

Parents will be made aware of the various ways in which their children may be at risk online, including, but not limited to:

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of pupils, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.
- Risks associated with generative artificial intelligence, including inappropriate content, manipulation, AI-generated imagery and the sharing of personal information

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 will be raised in the following ways:

- Newsletters
- Online resources
- Parent assembly during the week of Safer Internet Day

14. Internet access

All members of the school community will be 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 governing board will ensure the school's ICT network has appropriate filtering and monitoring systems in place and that it is meeting the DfE's Filtering and monitoring standards for schools and colleges. The governing board will also ensure that 'over-blocking' does not lead to unreasonable restrictions on what pupils can be taught in relation to online teaching and safeguarding.

The DSLs will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems so they meet the school's safeguarding needs.

The Headteacher, DSL and ICT Operations Manager will undertake an annual filtering and monitoring review to determine whether the systems remain appropriate and effective and meet the school's safeguarding needs. The review will include checks that filtering and monitoring operate appropriately across all internet-connected devices and relevant locations. A record of the review, identified risks and required actions will be retained and the outcome reported to the Governing Body.

As part of the annual review, the school will consider the safeguarding implications of emerging technologies, including generative AI. This will include consideration of whether the school's filtering and monitoring provision is able to identify and respond to real-time, dynamic, personalised and AI-generated content, where appropriate. The school will assess the risks associated with any generative AI products used or made available to pupils, with reference to the DfE's 'Generative AI: product safety standards.'

Managed digital monitoring: The school uses a fully managed digital monitoring system, Securus, provided by Capital Entrust. An external provider undertakes daily monitoring checks to ensure the systems remain effective and appropriate.

Alerting and triage of captures:

All "captures" (flagged events) are graded by Capital Entrust using the following scale:

1. False positive
2. Off task
3. Behaviour
4. Potential safeguarding concern (no immediate risk of harm)
5. Safeguarding concern with risk of immediate harm

The Headteacher (DDSL) and Assistant Headteacher (DDSL) are automatically emailed for all captures graded 3, 4 or 5. Grade 5 emails are always followed up with a phone call from the provider.

The Headteacher or Assistant Headteacher will investigate each notified capture. Where a capture involves racist or homophobic language or indicates a safeguarding concern, it will be added to MyConcern, a safeguarding log will be completed, and parents/carers will be contacted as appropriate.

Reporting and enforcement:

Reports of inappropriate websites or materials must be made to the ICT Operations Manager and DSLs immediately. They will investigate and make any necessary changes.

Deliberate breaches of the filtering system will be reported to the DSLs and ICT Operations Manager and escalated appropriately.

Pupils who deliberately breach the filtering system will be sanctioned in line with the Behaviour Policy.

Staff who deliberately breach the filtering system will be managed in line with the Disciplinary Policy and Procedure.

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

Transparency and data handling: The school's network and school-owned devices will be appropriately filtered and monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSLs and managed in line with the Child Protection and Safeguarding Policy.

Assurance and audit:

Half-termly, the Assistant Headteacher will cross-check graded captures as an additional layer of safeguarding oversight.

Once per term, the Assistant Headteacher and ICT Operations Manager will audit the device list to ensure Securus is installed and operating on all school-owned devices.

16. Network security

Technical security features, such as anti-virus software, will be kept up-to-date and managed by the ICT Operations Manager. Firewalls will be switched on at all times. The ICT Operations Manager will review the firewalls on a weekly basis to ensure they are running correctly, and to carry out any required updates.

Staff will be advised not to download unapproved software or open unfamiliar email attachments, and will be expected to report all malware and virus attacks to the ICT Operations Manager.

All members of staff will have their own unique usernames and private passwords to access the school's systems. Pupils KS2 will have their own unique username and year band specific passwords. Staff members will be responsible for keeping their passwords private. Passwords will have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible. Passwords will expire after 120 days, after which users will be required to change them.

Users will inform the ICT Operations Manager if they forget their login details, who will arrange for the user to access the systems under different login details. Users will not be permitted to share their login details with others and will not be 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 headteacher will be informed and will decide the necessary action to take.

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

17. Emails

Access to and the use of emails will be managed in line with the Data Protection Policy and the Acceptable Use Agreement.

Staff and pupils will be given approved school email accounts and will only be 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 and pupils must agree to and accept the Acceptable Use Agreement. Personal email accounts will not be permitted to be used on the school site. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Staff members and pupils will be required to block spam and junk mail, and report the matter to ICT Operations Manager. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened. Computing lessons where the use of email is required will explain what a phishing email and other malicious emails might look like – this will include information on the following:

- How to determine whether an email address is legitimate
- The types of address a phishing email could use
- The importance of asking “does the email urge you to act immediately?”
- The importance of checking the spelling and grammar of an email

18. Generative artificial intelligence (AI)

The school will take steps to prepare pupils for changing and emerging technologies, e.g. generative AI and how to use them safely and appropriately with consideration given to pupils' age.

The school will ensure its IT system includes appropriate filtering and monitoring systems to limit pupil's ability to access or create harmful or inappropriate content through generative AI.

The school will ensure that pupils are not accessing or creating harmful or inappropriate content, including through generative AI.

Staff and pupils must not enter personal, special-category, confidential or identifiable information into generative AI tools unless the tool has been specifically approved by the school and its use complies with the school's data-protection arrangements.

The school will make use of any guidance and support that enables it to have a safe, secure and reliable foundation in place before using more powerful technology such as generative AI.

Where generative AI products are used or made available to pupils, the school will assess their suitability and safeguarding risks, taking account of the DfE's 'Generative AI: product safety standards.' The school will consider risks relating to pupils' cognitive, emotional and social development, mental health, manipulation, privacy and exposure to inappropriate content.

19. Social networking

The use of social media by staff will be managed in line with the school's Computing Acceptable Use Policy.

20. The school website

The headteacher will be 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 will be managed in line with the School Website Policy.

21. Use of devices

Staff members and pupils will be issued with school-owned devices to assist with their work, where necessary. Requirements around the use of school-owned devices can be found in the school's Computing Acceptable Use Policy.

The use of personal devices on the school premises and for the purposes of school work will be managed in line with the Computing Acceptable Use Policy.

22. Remote learning

All remote learning will be delivered in line with the school's Blended and Remote Learning Policy. This policy specifically sets out how online safety will be considered when delivering remote education.

23. Monitoring and review

The school recognises that the online world is constantly changing; therefore, the DSL, DDSLs, computing lead and the headteacher conduct termly light-touch reviews of this policy to evaluate its effectiveness.

The governing board, headteacher and DSLs will review this policy in full on an annual basis and following any online safety incidents.

Any changes made to this policy are communicated to all members of the school community

