On-Line Safety Policy

Clipstone Brook Lower School

Created on:	January 2024	Sally Reay
Reviewed on:	February 2025	Sarah Orr
Next review by:	February 2026	

Contents:

Statement of Intent

Clipstone Brook Lower School understands that online services are essential to raising educational standards, promoting pupil achievement, and enhancing teaching and learning. Online services are embedded throughout the school; therefore, several controls are in place to ensure the safety of pupils and staff.

The breadth of issues classified within online safety is considerable. Still, 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 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 include online gambling, inappropriate advertising, phishing, and/or financial scams.

The measures implemented to protect pupils and staff revolve around these risk areas. Our school has created this policy to ensure 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:

- DfE (2023) 'Filtering and monitoring standards for schools and colleges'
- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE Keeping Children Safe in Education 2024
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- 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 (2018) 'Small Business Guide: Cyber Security'

This policy operates in conjunction with the following school policies:

- Social Media Policy
- Allegations of Abuse Against Staff Policy
- Child Protection and Safeguarding Policy
- Acceptable Use Agreement
- Data and Cyber-security Breach procedures-
- Child-on-child Abuse Policy
- Anti-Bullying Policy
- PSHE and RSE Policy
- Searching, Screening, and Confiscation procedure
- Mobile Phone and Internet Enabled Devices (Smart Watches) Policy
- Staff Code of Conduct Policy
- Behaviour Policy
- Disciplinary Policy and Procedures
- Data Protection Policy
- Confidentiality Policy
- Photography Procedure
- User Agreement Policy

2. Roles and responsibilities:

The governing board is responsible for:

- Ensuring this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL Team's remit covers online safety.
- Reviewing this policy annually.
- Ensuring their 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 the effectiveness of filtering and monitoring systems is reviewed annually in liaison with ICT staff and service providers.
- Ensure that the SLT and other relevant staff are aware and understand the filtering and monitoring provisions in place, manage them effectively, and know how to escalate concerns when identified.
- Ensuring that all relevant school policies have a practical approach to planning for and responding to online challenges and hoaxes embedded within them.

The headteacher is responsible for:

- Ensuring online safety is a running and interrelated theme throughout the school's policies and procedures, including those related to the curriculum, teacher training, and safeguarding.
- Supporting the DSL Team by ensuring they have enough time and resources to carry out their responsibilities regarding 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 understand online safety appropriately.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school keeps pupils safe.
- Working with the DSL and ICT technicians to conduct timely light-touch reviews of this policy.

The DSL Team 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 staff members on online safety matters
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and 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 and Termly Enrichment Days.
- Ensure that staff report online safety incidents and inappropriate internet use by pupils and staff.
- Maintaining records of reported online safety concerns and the actions taken in response to problems.
- Monitor online safety incidents to identify trends and gaps in the school's provision and use this data to update the school's procedures.
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that all safeguarding training given to staff includes understanding the expectations, roles, and responsibilities of filtering and monitoring systems at the school.
- Reporting to the governing board about online safety on a termly basis where required and instances occur.
- Working with ICT technicians to light-touch reviews of this policy.

ICT technicians are responsible for:

- Providing technical support in developing and implementing 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 appropriately.

All staff members are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or access.
- 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.
- Ensuring online safety is embedded in their curriculum teaching where relevant to their role.

Pupils are responsible for:

- Adhering to the Acceptable User Policy
- Seeking help from school staff if they are concerned about something they or a peer have experienced online.
- Reporting online safety incidents and concerns per this policy's procedures.

3. Managing online safety:

All staff will be aware that technology is a significant component in many safeguarding and well-being issues affecting young people, mainly owing to the rise of social media and the increased prevalence of children using the internet.
The DSL Team is responsible for the school's approach to online safety, with support from Senior Teachers where appropriate, and will ensure that robust processes are in place to handle any concerns about pupils' safety online. The DSL Team should liaise with the police or children's social care services for support in 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 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
- Assemblies/ Enrichment Days are conducted termly on remaining safe online.

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 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 harmful online sexual behaviour may ask for no one to be told about the abuse. The DSL Team will consider whether sharing details of the abuse would put the victim in a more harmful position or whether it is necessary to protect them from further harm. Ultimately, the DSL Team will balance the victim's wishes against their duty to protect the victim and other young people. The DSL Team and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures being put in place to support their child and how the report will progress.
Confidentiality will not be promised, and information may still be shared lawfully, for example, if the DSL decides 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, and appropriate support must be provided to the victim.
Concerns regarding a staff member's online behaviour are reported to the headteacher, who decides on the best course of action per the relevant policies, e.g., the Staff Code of Conduct, Allegations of Abuse Against Staff Policy, and Disciplinary Policy and Procedures. 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 DSL, which investigates concerns with relevant staff members, e.g., the headteacher and ICT technicians, and manages concerns by relevant policies depending on their nature, e.g., the Behaviour Policy and Child Protection and Safeguarding Policy.
Where there is a concern about illegal activity, the 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 Child Protection and Safeguarding Policy. The Safeguarding Hub at CBC will be contacted to discuss if the DSL Team deems this helpful to discuss.
The DSL Team records all online safety incidents and the school's response.

4. 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 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, mainly if they are using websites that they know adults will consider 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 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 offense, 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 harmful online 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 repeated harassment. The school will respond to these incidents. 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 Team, 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 to manipulate, exploit, and/or abuse 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 talking to an adult masquerading as someone younger to gain their trust to abuse them.
- The pupil does not want to admit to talking to someone they met online for fear of judgement, embarrassment, or a lack of understanding from their peers or adults.
- The pupil may have been manipulated into 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,' mainly 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, love, fear, distress, and confusion.

Due to the fact pupils are less likely to report grooming than other online offenses, staff must understand the indicators of this type of abuse. The DSL Team will ensure that online safety training covers online abuse, the importance of looking for signs of grooming, and the signs of online grooming, including

- Being secretive about how they spend their time.
- Having an older boyfriend or girlfriend, usually one that does not attend 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 and 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 the broader 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 severe 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 about CSE or CCE, they will bring these concerns to the DSL Team without delay, who will manage the situation in line with the Child Protection and Safeguarding Policy.

Radicalisation

is the process by which a person supports 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 to involve 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 that can place 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.
When staff is concerned about a pupil relating to radicalisation, they will report this to the DSL Team without delay, who will handle the situation in line with the Prevent Duty procedure outlined in the Safeguarding Policy.

7. Mental health

The internet, particularly social media, can be the root cause of several 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 substantially impact a pupil's mental state positively and negatively. The DSL will ensure that training is available to help staff members understand popular social media sites and terminology, how 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 a pupil's mental health will be addressed per the SEND Policy.

8. Online hoaxes and harmful online challenges

For this policy, an **"online hoax"** is defined as a deliberate lie designed to seem truthful, customarily intended to scaremonger or distress individuals who come across it, and spread on social media platforms.
For this policy, **"harmful online challenges"** refers to challenges 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 how 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 Team immediately.
The DSL Team 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 localised to the school or the local area or 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.
Before deciding how to respond to a harmful online challenge or hoax, the DSLs and the headteacher will decide whether each proposed response is:

- This aligns with any advice 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 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 DSL team'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 DSL Team and headteacher will only implement a school-wide approach to highlighting the 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. Cyber-crime

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

- **Cyber-enabled** – these crimes can be carried out offline; however, are made more manageable 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 in cybercrime, whether deliberately or inadvertently. Where there are any concerns about a pupil’s use of technology and their intentions about using their skill and affinity towards it, the DSL Team 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 Team and headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly, and lawfully. They 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 school networks through appropriate firewalls.

10. Online safety training for staff

The DSL 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.

11. Online safety and the curriculum

Online safety is embedded throughout the curriculum; however, it is mainly addressed in the following subjects:

- Relationships between Sexual Education (RSE) and Personal, Social, and Health Education (PSHE)
- 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 navigate the online world safely and confidently regardless of their device, platform, or app. 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 risks pupils may face online are always considered when developing the curriculum. The risks considered and how they are covered in the curriculum can be found in appendix A of this policy.
The DSL is involved with developing 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.
The school recognises that, while any pupil can be vulnerable online, some pupils 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 LAC. Relevant staff members, e.g., the SENCO and designated teacher for LAC, 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 teach about online safety for more susceptible children and in response to instances of harmful online behaviour from pupils.
Class teachers review external resources before using them for the online safety curriculum to ensure they are appropriate for the cohort of pupils. When examining these resources, the following questions are asked:

- Where does this organisation get its 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?

External visitors may be invited into the school to help deliver certain aspects of the online safety curriculum. The headteacher and DSL Team will decide when to ask external groups into the school and ensure the selected visitors are appropriate.
Before conducting a lesson or activity on online safety, the class teacher and DSL Team consider the topic 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 Team will advise the staff member/s on how to support best any pupil whom a lesson or activity may significantly impact. 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 saying what they feel and asking 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.

Suppose a pupil discloses to a staff member about online abuse following a lesson or activity. In that case, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

12. Use of technology in the classroom

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

- Computers
- Laptops
- Tablets
- Intranet
- Email
- Cameras

Before using any websites, tools, apps, or other online platforms in the classroom or recommending pupils use these platforms at home, the class teacher constantly 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 for their age and ability.

13. 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 that 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 User Agreement for Pupils.
Pupils will not be permitted to use smart devices or other personal technology in the classroom or school.
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 properly.

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.

14. Educating Parents and/or Carers:

The school works with parents to ensure pupils stay safe online and at home. Parents are provided with information about the school's approach to online safety and their role in protecting their children. Parents can access a copy of the

Acceptable Use Agreement and are encouraged to go through this with their child where it is deemed age-appropriate.
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.

Parents will be informed of how 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:

- Pupils run parents' session/s in KS1 and KS2 and are age-appropriate.
- Newsletters (where relevant)
- Online resources

15. Internet access:

All school community members 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 use the internet appropriately.

16. Filtering and monitoring online activity

The governing board will ensure the school's ICT network has appropriate filters and monitoring systems and meets the DfE's 'Filtering and monitoring standards for schools and colleges'. The governing board will ensure 'overblocking' does not lead to unreasonable restrictions on what pupils can be taught about online teaching and safeguarding.

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

The headteacher and ICT technicians will assess risk to determine the required filtering and monitoring systems. The school's filtering and monitoring systems will be 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. ICT

technicians will undertake monthly checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system will be directed to the headteacher. Before making any changes to the filtering system, ICT technicians and the DSL will conduct a risk assessment. ICT technicians will record any changes made to the system. Reports of inappropriate websites or materials will be made to the DSL, who will review them with the ICT technician to investigate the matter and make any necessary changes immediately.

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

Suppose material 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 will be appropriately 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 DSL, who will manage the situation in line with the Child Protection and Safeguarding Policy.

17. Network security

Technical security features, such as anti-virus software, are kept up-to-date and managed by ICT technicians. Firewalls are switched on at all times. ICT technicians review the firewalls monthly to ensure they are running correctly and to perform 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 ICT technicians.
All staff members have unique usernames and private passwords to access the school's systems. Pupils are provided usernames and passwords in class, year. . Staff members 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.
Users inform ICT technicians if they forget their login details, who will arrange for the user to access the systems under different login details. Users cannot share their login details with others and cannot 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 is informed and decides the necessary action to take.
Users must lock access to devices and systems when not in use.

18. Emails

Access to and the use of emails is managed in line with the Data Protection Policy and Acceptable Use Agreement. Staff and pupils are given approved school email accounts and can only use these accounts at school and when doing school-related work outside school hours. Personal email accounts are not permitted to be used on the school site. Any email that contains sensitive or confidential information is only sent using a secure and encrypted email or platform.

Staff members and pupils must block spam and junk mail and report the matter to ICT technicians. 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 emails from unknown sources are deleted without being opened.

Any cyber-attacks initiated through emails are managed per the Data and Cyber-security Breach Prevention and Management Plan.

19. 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. Staff can use personal social media during break and lunchtimes; however, inappropriate or excessive use during school hours may result in removing internet access or further action. Staff members are advised that their social media conduct can impact their role and reputation within the school. The Staff Code of Conduct contains information on the acceptable use of social media – staff members must always follow these expectations.

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 cannot contact them on social media. Where a member of staff has an existing personal relationship with a parent or pupil and thus is connected with them on social media, e.g., they are friends with a parent at the school; they will disclose this to the headteacher. They will ensure that their social media conduct relating to that parent is appropriate for their position in the school.

The online safety curriculum teaches Pupils how to use social media safely and responsibly.

Concerns regarding the online conduct of any member of the school community on social media are reported to the DSL and managed by the relevant policy, e.g., the Anti-Bullying Policy, Staff Code of Conduct, and Behaviour Policy.

Use on behalf of the school.

The use of social media on behalf of the school is conducted in line with the Social Media Policy. The school's official social media channels are only used for educational or engagement purposes. Staff members must be authorised by the headteacher to access the school's social media accounts.

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

20. The school website

The 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 publication guidelines, including accessibility, data protection, respect for intellectual property rights, privacy policies, and copyright law.
Personal information relating to staff and pupils should be published on the website.
Images and videos are only posted on the website if the provisions in the Photography Policy are met.

21. Use of devices

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

- Laptop

Pupils are provided with school-owned devices to assist in the curriculum delivery, e.g., laptops to use during lessons.
Staff and pupils need help connecting school-owned devices to public Wi-Fi networks. All school-owned devices are fitted with software to ensure they can be remotely accessed if data needs to be protected, retrieved, or erased.
ICT technicians review all school-owned devices regularly to update software and ensure no inappropriate material or malware on the devices. Software, apps, or other programmes can only be downloaded onto a device with authorisation from ICT technicians.

Cases of staff members or pupils found to be misusing school-owned devices will be managed in line with the Behaviour Policy, respectively.

Personal devices

Any personal electronic device brought into school is the user's responsibility.
Staff members are not permitted to use their devices during lesson time other than in an emergency. Staff members are not permitted to use their devices to take photos or videos of pupils.
Staff members report concerns about their colleagues' use of personal devices on the school premises in line with the Allegations of Abuse Against Staff Policy. If a staff member is thought to have illegal content saved or stored on a personal device or to have committed an offence using a personal device, the headteacher will inform the police, and action will be taken in line with the Allegations of Abuse Against Staff Policy.
The headteacher may authorise the use of mobile devices by a pupil for safety or precautionary use and rules for conduct are developed and managed on a case-by-case basis.
Pupils' devices can be searched, screened, and confiscated. If a staff member reasonably believes a pupil's device has been used to commit an offence or may provide evidence relating to an offence, the device will be handed to the police.

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 Team.

22.Monitoring and review

The school recognises that the online world is constantly changing; therefore, the DSL Team, ICT technicians, and the headteacher conduct timely light-touch reviews of this policy to evaluate its effectiveness.
The governing board, 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 Jan 26.
Any changes made to this policy are communicated to all school community members.

Online harms and risks – curriculum coverage

Please note that reference has been made to KS3 and KS4 which are covered at Secondary Aged Curriculum and not Primary (EYFS, KS1 and KS2)

Subject area	Description and teaching content	Curriculum area the harm or risk is covered in
How to navigate the internet and manage information		
Age restrictions	Some online activities have age restrictions because they include content which is not appropriate for children under a specific age. Teaching includes the following: • That age verification exists and why some online platforms ask users to verify their age • Why age restrictions exist • That content that requires age verification can be damaging to under-age consumers • What the age of digital consent is (13 for most platforms) and why it is important	This risk or harm is covered in the following curriculum areas: • PSHE • Computing
How content can be used and shared	Knowing what happens to information, comments or images that are put online. Teaching includes the following: • What a digital footprint is, how it develops and how it can affect pupils' futures • How cookies work • How content can be shared, tagged and traced • How difficult it is to remove something once it has been shared online • What is illegal online, e.g. youth-produced sexual imagery (sexting)	This risk or harm is covered in the following curriculum areas: • Relationships education • Computing
Disinformation, misinformation and hoaxes	Some information shared online is accidentally or intentionally wrong, misleading or exaggerated. Teaching includes the following: • Disinformation and why individuals or groups choose to share false information in order to deliberately deceive • Misinformation and being aware that false and misleading information can be shared inadvertently	This risk or harm is covered in the following curriculum areas: • Relationships and health education • KS2 Computing

	● Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons ● That the widespread nature of this sort of content can often appear to be a stamp of authenticity, making it important to evaluate what is seen online ● How to measure and check authenticity online ● The potential consequences of sharing information that may not be true	
Fake websites and scam emails	Fake websites and scam emails are used to extort data, money, images and other things that can either be used by the scammer to harm the person targeted or sold on for financial, or other, gain. Teaching includes the following: ● How to recognise fake URLs and websites ● What secure markings on websites are and how to assess the sources of emails ● The risks of entering information to a website which is not secure ● What pupils should do if they are harmed, targeted, or groomed as a result of interacting with a fake website or scam email ● Who pupils should go to for support	This risk or harm is covered in the following curriculum areas: ● Relationships education ● Computing
Online fraud	Fraud can take place online and can have serious consequences for individuals and organisations. Teaching includes the following: ● What identity fraud, scams and phishing are ● That children are sometimes targeted to access adults' data ● What 'good' companies will and will not do when it comes to personal details	This risk or harm is covered in the following curriculum areas: ● Relationships education ● Computing
Password phishing	Password phishing is the process by which people try to find out individuals' passwords so they can access protected content. Teaching includes the following: ● Why passwords are important, how to keep them safe and that others might try to get people to reveal them ● How to recognise phishing scams	This risk or harm is covered in the following curriculum areas: ● Relationships education ● Computing

	● The importance of online security to protect against viruses that are designed to gain access to password information ● What to do when a password is compromised or thought to be compromised	
Personal data	Online platforms and search engines gather personal data – this is often referred to as 'harvesting' or 'farming'. Teaching includes the following: ● How cookies work ● How data is farmed from sources which look neutral ● How and why personal data is shared by online companies ● How pupils can protect themselves and that acting quickly is essential when something happens ● The rights children have with regards to their data ● How to limit the data companies can gather	This risk or harm is covered in the following curriculum areas: ● Relationships education ● Computing
Persuasive design	Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. Teaching includes the following: ● That the majority of games and platforms are designed to make money, and that their primary driver is to encourage people to stay online for as long as possible ● How notifications are used to pull users back online	This risk or harm is covered in the following curriculum areas: ● Computing
Privacy settings	Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared. Teaching includes the following: ● How to find information about privacy settings on various devices and platforms ● That privacy settings have limitations	This risk or harm is covered in the following curriculum areas: ● Relationships education ● Computing

Targeting of online content	Much of the information seen online is a result of some form of targeting. Teaching includes the following: ● How adverts seen at the top of online searches and social media have often come from companies paying to be on there and different people will see different adverts ● How the targeting is done ● The concept of clickbait and how companies can use it to draw people to their sites and services	This risk or harm is covered in the following curriculum areas: ● Relationships education ● Computing
How to stay safe online		
Online abuse	Some online behaviours are abusive. They are negative, potentially harmful, and, in some cases, can be illegal. Teaching includes the following: ● The types of online abuse, including sexual harassment, bullying, trolling, and intimidation ● When online abuse can become illegal ● How to respond to online abuse and how to access support ● How to respond when the abuse is anonymous ● The potential implications of online abuse ● What acceptable and unacceptable online behaviours look like	This risk or harm is covered in the following curriculum areas: ● Relationships education ● Computing
Challenges	Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching includes the following: ● What an online challenge is and that, while some will be fun and harmless, others may be dangerous and even illegal ● How to assess if the challenge is safe or potentially harmful, including considering who has generated the challenge and why ● That it is okay to say no and to not take part in a challenge ● How and where to go for help	This risk or harm is covered in the following curriculum areas: ● Relationships education

	● The importance of telling an adult about challenges which include threats or secrecy, such as 'chain letter' style challenges	
Content which incites violence	Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching includes the following: ● That online content (sometimes gang related) can glamorise the possession of weapons and drugs ● That to intentionally encourage or assist in an offence is also a criminal offence ● How and where to get help if they are worried about involvement in violence	This risk or harm is covered in the following curriculum areas: ● Relationships education
Fake profiles	Not everyone online is who they say they are. Teaching includes the following: ● That, in some cases, profiles may be people posing as someone they are not or maybe 'bots' ● How to look out for fake profiles	This risk or harm is covered in the following curriculum areas: ● Relationships education ● Computing
Grooming	Knowing about the different types of grooming and motivations for it, e.g., radicalisation, child sexual abuse and exploitation, and gangs and county lines. Teaching includes the following: ● Boundaries in friendships with peers, in families, and with others ● Key indicators of grooming behaviour ● The importance of disengaging from contact with suspected grooming and telling a trusted adult ● How and where to report grooming both in school and to the police At all stages, it is important to balance teaching pupils about making sensible decisions to stay safe while being clear it is never the fault of the child who is abused and why victim blaming is always wrong.	This risk or harm is covered in the following curriculum areas: ● Relationships education

Livestreaming	Livestreaming (showing a video of yourself in real-time online, either privately or to a public audience) can be popular with children, but it carries a risk when carrying out and watching it. Teaching includes the following: ● What the risks of carrying out live streaming are, e.g., the potential for people to record live streams and share the content ● The importance of thinking carefully about who the audience might be and if pupils would be comfortable with whatever they are streaming being shared widely ● That online behaviours should mirror offline behaviours and that this should be considered when making a livestream ● those pupils should not feel pressured to do something online that they would not do offline ● Why people sometimes do and say things online that they would never consider appropriate offline ● The risk of watching videos that are being live-streamed, e.g. there is no way of knowing what will be shown next ● The risks of grooming	This risk or harm is covered in the following curriculum areas: ● KS3 and 4 RSHE
Pornography	Knowing that sexually explicit material presents a distorted picture of sexual behaviours. Teaching includes the following: ● That pornography is not an accurate portrayal of adult sexual relationships ● That viewing pornography can lead to skewed beliefs about sex and, in some circumstances, can normalise violent sexual behaviour ● That not all people featured in pornographic material are doing so willingly, i.e., revenge porn or people trafficked into sex work	This risk or harm is covered in the following curriculum areas: ● KS3 and 4 RSHE
Unsafe communication	Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching includes the following:	This risk or harm is covered in the following curriculum areas:

	● That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with ● How to identify indicators of risk and unsafe communications ● The risks associated with giving out addresses, phone numbers or email addresses to people pupils do not know, or arranging to meet someone they have not met before ● What online consent is and how to develop strategies to confidently say no to both friends and strangers online	● Relationships education ● Computing
Wellbeing		
Impact on confidence (including body confidence)	Knowing about the impact of comparisons to 'unrealistic' online images. Teaching includes the following: ● The issue of using image filters and digital enhancement ● The role of social media influencers, including that they are paid to influence the behaviour of their followers ● The issue of photo manipulation, including why people do it and how to look out for it	This risk or harm is covered in the following curriculum areas: ● KS3 and 4 RSHE
Impact on quality of life, physical and mental health and relationships	Knowing how to identify when online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent online and offline. Teaching includes the following: ● How to evaluate critically what pupils are doing online, why they are doing it, and for how long (screen time) ● How to consider quality vs. quantity of online activity ● The need for pupils to consider if they are enjoying being online or just doing it out of habit, due to peer pressure or due to the fear or missing out ● That time spent online gives users less time to do other activities, which can lead some users to become physically inactive	This risk or harm is covered in the following curriculum areas: PSHE Curriculum

	● The impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues ● That isolation and loneliness can affect pupils and that it is very important for them to discuss their feelings with an adult and seek support ● Where to get help	
Online vs. offline behaviours	People can often behave differently online to how they would act face to face. Teaching includes the following: ● How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressures around having perfect or curated lives ● How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face	This risk or harm is covered in the following curriculum areas: ● Relationships education
Reputational damage	What users post can affect future career opportunities and relationships – both positively and negatively. Teaching includes the following: ● Strategies for positive use ● How to build a professional online profile	This risk or harm is covered in the following curriculum areas: ● RSHE at KS3 and KS4
Suicide, self-harm, and eating disorders	Pupils may raise topics including eating disorders, self-harm and suicide. Teachers must be aware of the risks of encouraging or making these seem a more viable option for pupils. They should take care to avoid giving instructions or methods and avoid using language, videos, and images.	As issues arise