



Online Safety Policy

Contents:

Statement of intent	
1. Legal framework	2
2. Roles and responsibilities	3
3. The curriculum	6
4. Staff training	8
5. Educating parents	9
6. Classroom use	9
7. Filtering and monitoring online activity	10
8. Network security	11
9. Emails	12
10. Personal use	13
11. The school website	14
12. Use of school-owned devices	14
13. Use of personal devices	15
14. Managing reports of online safety incidents	14
15. Responding to specific online safety concerns	16
16. Remote Learning	19
17. Monitoring and review	21
<i>Appendices</i>	
Appendix 1 – Online Safety Curriculum	22
Appendix 2 – Online harms and risks – curriculum coverage	23

Statement of intent

St Stephen's CE Primary understands that using online services is an important aspect of raising educational standards, promoting pupil achievement and enhancing teaching and learning.

The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

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

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

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

1. Legal framework

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

- Voyeurism (Offences) Act 2019
- The General Data Protection Regulation (GDPR)
- Data Protection Act 2018
- DfE (2023) 'Keeping children safe in education'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- National Cyber Security Centre (2017) 'Cyber Security: Small Business Guide'

- UK Council for Child Internet Safety (2017) 'Sexting in schools and colleges: Responding to incidents and safeguarding young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'

1.2. This policy operates in conjunction with the following school policies:

- Cyberbullying Policy
- Allegations of Abuse Against Staff Policy
- ICT Acceptable Use Policy
- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- PSHE Policy
- RSE Policy
- Staff Code of Conduct and Handbook
- Behaviours Policy
- Disciplinary Policy and Procedures
- Data Protection Policy
- Prevent Duty Policy

2. Roles and responsibilities

2.1. The governing body is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's 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 and governors undergo safeguarding and child protection training (including online safety) at induction.
- 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.

2.2. The headteacher is responsible for:

- Supporting the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL and governing body to update this policy on an annual basis.

2.3. The DSL is responsible for:

- Taking the lead responsibility for online safety in the school.
- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring appropriate referrals are made to external agencies, as required.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Staying up-to-date with current research, legislation and online trends.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.

- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
- Ensuring all members of the school community understand the reporting procedure.
- 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.
- Reporting to the governing body about online safety on a termly basis.
- Working with the headteacher and governing body to update this policy on an annual basis.

2.4. ICT technicians are responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

2.5. All staff members are responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- 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.

2.6. Pupils are responsible for:

- Adhering to this policy, the ICT Acceptable Use Policy and other relevant policies.
- Seeking help from school staff if they are concerned about something they or a peer has experienced online.
- Reporting online safety incidents and concerns in line with the procedures within this policy.

3. The curriculum

- 3.1. Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:
 - Computing
 - PSHE
 - Relationships and Health Education
- 3.2. The curriculum and the school's approach to online safety is developed in line with the UK Council for Child Internet Safety's 'Education for a Connected World' framework and the DfE's 'Teaching online safety in school' guidance. We use materials produced by National Online Safety in order to deliver the curriculum.
- 3.3. 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.
- 3.4. Online safety teaching is always appropriate to pupils' ages and developmental stages.
- 3.5. 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
- 3.6. The online risks pupils may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in Part 2 of this policy.

- 3.7. The DSL is involved with the development of the school's online safety curriculum.
- 3.8. The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and LAC. Relevant members of staff, 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.
- 3.9. Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils. When reviewing these resources, the following questions are asked:
- Where does this organisation get their information from?
 - What is their evidence base?
 - Have they been externally quality assured?
 - What is their background?
 - Are they age appropriate for pupils?
 - Are they appropriate for pupils' developmental stage?
- 3.10. External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The headteacher and DSL decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.
- 3.11. Before conducting a lesson or activity on online safety, the class teacher and DSL consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL advises the staff member on how to best support any pupil who may be especially impacted by a lesson or activity.
- 3.12. 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.
- 3.13. During an online safety lesson or activity, the class teacher ensures a safe environment is maintained in which pupils feel comfortable to say what they feel and are not worried about getting into trouble or being judged.
- 3.14. If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with sections 14 and 15 of this policy.

- 3.15. 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 sections 14 and 15 of this policy.

4. Staff training

- 4.1. All staff receive safeguarding and child protection training, which includes online safety training, during their induction.
- 4.2. Online safety training for staff is updated annually and is delivered in line with advice from the three local safeguarding partners.
- 4.3. In addition to this training, staff also receive regular online safety updates as required and at least annually.
- 4.4. The DSL and any deputies undergo training to provide them with the knowledge and skills they need to carry out their role, this includes online safety training. This training is updated at least every two years.
- 4.5. 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.
- 4.6. In addition to this formal training, the DSL and any deputies receive regular online safety updates to allow them to keep up with any developments relevant to their role. In relation to online safety, these updates allow the DSL and their deputies to:
- Understand the unique risks associated with online safety and be confident that they have the relevant knowledge and capability required to keep pupils safe while they are online at school.
 - Recognise the additional risks that pupils with SEND face online and offer them support to stay safe online.
- 4.7. All staff receive a copy of this policy upon their induction and are informed of any changes to the policy.
- 4.8. Staff are required to adhere to the Staff Code of Conduct and Handbook; and ICT Acceptable Use Policy at all times, which includes provisions for the acceptable use of technologies and the use of social media.
- 4.9. All staff are informed about how to report online safety concerns, in line with sections 14 and 15 of this policy.

- 4.10. The DSL acts as the first point of contact for staff requiring advice about online safety.

5. Educating parents

- 5.1. The school works in partnership with parents to ensure pupils stay safe online at school and at home.
- 5.2. Parents are provided with information about the school's approach to online safety and their role in protecting their children. Parental awareness is raised in the following ways:
- Through use of school's subscription to National Online Safety (NOS), and reminders about the resources this contains
 - Through the school website
 - Leaflets, including NOS 'Guides'
 - Newsletters/Homelink
- 5.3. Parents are sent a copy of the Pupils' ICT Acceptable Use Policy 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.

6. Classroom use

- 6.1. A wide range of technology is used during lessons, including the following:
- Computers
 - Laptops
 - Tablets
 - Internet
 - Email
 - Cameras
- 6.2. Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher always reviews and evaluates the resource.
- 6.3. Class teachers ensure that any internet-derived materials are used in line with copyright law.
- 6.4. Pupils are closely supervised when using online materials during lesson time – this supervision is suitable to their age and ability.

7. Filtering and monitoring online activity

- 7.1. The governing board will ensure the school's ICT network has appropriate filters 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 ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding. The headteacher and ICT technicians undertake a risk assessment to determine what filtering and monitoring systems are required.
- 7.2. 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.
- 7.3. The filtering and monitoring systems the school implements are appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks.
- 7.4. The governing body ensures 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.
- 7.5. ICT technicians undertake regular checks on the filtering and monitoring systems to ensure they are effective and appropriate.
- 7.6. Requests regarding making changes to the filtering system are directed to the headteacher.
- 7.7. Any changes made to the system are recorded by ICT technicians.
- 7.8. Reports of inappropriate websites or materials are made to an ICT technician immediately, who investigates the matter and makes any necessary changes.
- 7.9. Deliberate breaches of the filtering system are reported to the DSL and ICT technicians, who will escalate the matter appropriately.
- 7.10. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviours Policy.
- 7.11. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.
- 7.12. If material that is believed to be illegal is accessed, inadvertently or deliberately, this material will be reported to the appropriate agency immediately, e.g. the Internet Watch Foundation (IWF), CEOP and/or the police.
- 7.13. The school's network of desktop and laptop computers are appropriately monitored as follows:

- The ICT Technician receives alerts of pupils' breaches to the filtering system or use of 'trigger words' using appropriate software. The ICT Technician in turn filters out 'false positives' and alerts the DSL to positive breaches who then responds appropriately. Alerts that need following up are recorded on CPOMS.
- The DSL receives alerts to all staff breaches of the filtering system, or use of 'trigger words', using appropriate software. All 'false positives' are noted as such, and any deliberate breach or cause for concern will be discussed with the Headteacher who will decide appropriate action.
- The headteacher will receive and investigate DSL breaches or alerts of the filtering system, or use of 'trigger words'.
- All users of the network and school-owned devices are informed about how and why they are monitored, through the ICT Acceptable Use Policy.

8. Network security

- 8.1. Technical security features, such as anti-virus software, are kept up-to-date and managed by ICT technicians.
- 8.2. Firewalls are switched on at all times.
- 8.3. ICT technicians review the firewalls on a weekly basis to ensure they are running correctly, and to carry out any required updates.
- 8.4. Staff and pupils are advised not to download unapproved software or open unfamiliar email attachments.
- 8.5. Staff members and pupils report all malware and virus attacks to ICT technicians.
- 8.6. All members of staff have their own unique usernames and private passwords to access the school's systems.
- 8.7. Pupils in each class are provided with their own unique username and private passwords.
- 8.8. Staff members and pupils are responsible for keeping their passwords private.
- 8.9. Passwords have a minimum and maximum length and should be a mixture of letters, numbers and symbols to ensure they are as secure as possible.
- 8.10. Users are not permitted to share their login details with others and are not allowed to log in as another user at any time.

- 8.11. Users are required to lock access to devices and systems when they are not in use.
- 8.12. Users inform ICT technicians if they forget their login details, who will arrange for the user to access the systems under different login details.
- 8.13. 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.

9. Emails

- 9.1. Access to and the use of emails is managed in line with the Data Protection Policy and ICT Acceptable Use Policy
- 9.2. Staff are given approved school email accounts and are only permitted to use these accounts at school and when doing school-related work outside of school hours.
- 9.3. Prior to being authorised to use the email system, staff must agree to and sign the relevant ICT Acceptable Use Policy.
- 9.4. Personal email accounts are not permitted to be used via the school network.
- 9.5. Any email that contains sensitive or personal information is only sent using secure and encrypted email.
- 9.6. Staff members and pupils are required to block spam and junk mail, and report the matter to ICT technicians.
- 9.7. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff are made aware of this.
- 9.8. Chain letters, spam and all other emails from unknown sources are deleted without being opened.
- 9.9. Online safety lessons include explanations of what phishing emails and other malicious emails might look like, including 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

10. Personal use

- 10.1. Access to social networking sites is filtered as appropriate.
- 10.2. Staff and pupils are not permitted to use social media for personal use during lesson time.
- 10.3. Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school.
- 10.4. Staff are not permitted to communicate with pupils or parents over social networking sites and are reminded to alter their privacy settings to ensure pupils and parents are not able to contact them on social media.
- 10.5. Pupils are taught how to use social media safely and responsibly through the online safety curriculum.
- 10.6. Concerns regarding the online conduct of any member of the school community on social media are reported to the Headteacher or DSL and managed in accordance with the relevant policy, e.g. Anti-Bullying Policy, Staff Code of Conduct and Behaviours Policy.
- 10.7. Use on behalf of the school
 - The use of social media on behalf of the school is conducted in line with the ICT Acceptable Use Policy.
 - The school's official social media channels are only used for official educational or engagement purposes.
 - Staff members must be authorised by the headteacher to access to 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.
 - The ICT Acceptable Use Policy contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.

11. The school website

- 11.1. 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.
- 11.2. The website complies with guidelines for publications including accessibility, data protection, respect for intellectual property rights, privacy policies and copyright law.

- 11.3. Personal information relating to staff and pupils is not published on the website.
- 11.4. Images and videos are only posted on the website if permissions have been given from parents/carers.

12. Use of school-owned devices

- 12.1. Appropriate staff members are issued with the laptops to assist with their work.
- 12.2. Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g. tablets to use during lessons.
- 12.3. Staff and pupils are not permitted to connect school-owned devices to public Wi-Fi networks without the permission of the head teacher.
- 12.4. All school-owned devices are fitted with software to ensure they can be remotely accessed, in case data on the device needs to be protected or retrieved.
- 12.5. ICT technicians review all school-owned devices regularly to carry out software updates and ensure there is no inappropriate material on the devices.
- 12.6. Staff members or pupils found to be misusing school-owned devices are disciplined in line with the Disciplinary Policy and Procedure and Behaviours Policy.

13. Use of personal devices

- 13.1. Any personal electronic device, including mobile phones, that is brought into school is the responsibility of the user.
- 13.2. Pupils are not permitted to bring a personal device onto school premises.
- 13.3. Personal devices, including mobile phones, are not permitted to be used in school other than during lunchtime or break. There must be no children present if your personal device is used at this time.
- 13.4. Members of the Leadership Team, DSL/DDSLs or site manager are permitted to carry their mobile device, for safeguarding reasons, as they may need to be contacted immediately in case of emergency. The use of this mobile device during working hours should be for school related use only.
- 13.5. Staff members are not permitted to use their personal devices during lesson time. If there is an emergency, the class or office telephone should be used.

- 13.6. Staff members are not permitted to use their personal devices to take photos or videos of pupils.
- 13.7. 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 or the Low Level Concerns Policy.
- 13.8. If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the headteacher will inform the police and action will be taken in line with the Allegations of Abuse Against Staff Policy.
- 13.9. Pupils may not bring their own personal devices into school. If a pupil needs to contact their parents during the school day, they may use the phone in the school office.
- 13.10. Pupils' devices can be searched, screened and confiscated in accordance with the Searching, Screening and Confiscation Policy.
- 13.11. If a staff member reasonably believes a pupil's personal device has been used to commit an offence or may provide evidence relating to an offence, the device will be handed to the police.
- 13.12. Appropriate signage is displayed to inform visitors to the school of the expected use of personal devices.
- 13.13. Any concerns about visitors' use of personal devices on the school premises are reported to the DSL or Headteacher.

14. Managing reports of online safety incidents

- 14.1. Staff members and pupils are informed about what constitutes inappropriate online behaviour in the following ways:
 - Staff training
 - The online safety curriculum
 - Collective Worship
- 14.2. 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, e.g. Staff Code of Conduct, Allegations of Abuse Against Staff Policy and Disciplinary Policy and Procedures.

- 14.3. Concerns regarding a pupil's online behaviour are reported to the DSL who investigates concerns with relevant staff members, e.g. the headteacher and ICT technicians. Concerns and actions taken will be recorded on CPOMS.
- 14.4. Concerns regarding a pupil's online behaviour are dealt with in accordance with relevant policies depending on their nature, e.g. Behaviours Policy and Child Protection and Safeguarding Policy.
- 14.5. Where there is a concern that illegal activity has taken place, the headteacher contacts the police.
- 14.6. All online safety incidents and the school's response are recorded by the DSL.

15. Responding to specific online safety concerns

Cyberbullying

- 15.1. Cyberbullying, against both pupils and staff, is not tolerated.
- 15.2. Any incidents of cyberbullying are dealt with quickly and effectively whenever they occur.
- 15.3. Information about the school's full response to incidents of cyberbullying can be found in the Cyberbullying Policy.

Online sexual violence and sexual harassment between children (child-on-child abuse)

- 15.4. The school recognises that child-on-child abuse can take place online. Examples include the following:
 - Non-consensual sharing of sexual images and videos
 - Sexualised cyberbullying
 - Online coercion and threats
 - Unwanted sexual comments and messages on social media
 - Online sexual exploitation
- 15.5. The school responds to all concerns regarding online child-on-child abuse, whether or not the incident took place on the school premises or using school-owned equipment.
- 15.6. Concerns regarding online child-on-child abuse are reported to the DSL who will investigate the matter in line with the Child Protection and Safeguarding Policy.

- 15.7. Information about the school's full response to incidents of online peer-on-peer abuse can be found in the Child Protection and Safeguarding Policy.

Upskirting

- 15.8. Under the Voyeurism (Offences) Act 2019, it is an offence to operate equipment and to record an image beneath a person's clothing without consent and with the intention of observing, or enabling another person to observe, the victim's genitals or buttocks (whether exposed or covered with underwear), in circumstances where their genitals, buttocks or underwear would not otherwise be visible, for a specified purpose.
- 15.9. A "specified purpose" is namely:
- Obtaining sexual gratification (either for themselves or for the person they are enabling to view the victim's genitals, buttocks or underwear).
 - To humiliate, distress or alarm the victim.
- 15.10. "Operating equipment" includes enabling, or securing, activation by another person without that person's knowledge, e.g. a motion activated camera.
- 15.11. Upskirting is not tolerated by the school.
- 15.12. Incidents of upskirting are reported to the DSL who will then decide on the next steps to take, which may include police involvement, in line with the Child Protection and Safeguarding Policy.

Youth produced sexual imagery (sexting)

- 15.13. Youth produced sexual imagery is the sending or posting of sexually suggestive images of under-18s via mobile phones or over the internet. Creating and sharing sexual photos and videos of individuals under 18 is illegal.
- 15.14. All concerns regarding sexting are reported to the DSL.
- 15.15. Following a report of sexting, the following process is followed:
- The DSL holds an initial review meeting with appropriate school staff
 - Subsequent interviews are held with the pupils involved, if appropriate
 - Parents are informed at an early stage and involved in the process unless there is a good reason to believe that involving the parents would put the pupil at risk of harm

- At any point in the process if there is a concern a pupil has been harmed or is at risk of harm, a referral will be made to children's social care services and/or the police immediately
 - The interviews with staff, pupils and their parents are used to inform the action to be taken and the support to be implemented
- 15.16. When investigating a report, staff members must not view the youth produced sexual imagery – this is an offence.
- 15.17. Any accidental or intentional viewing of youth produced sexual imagery must be recorded, and the headteacher or DSL informed

Online abuse and exploitation

- 15.18. Through the online safety curriculum, pupils are taught about how to recognise online abuse and where they can go for support if they experience it.
- 15.19. The school responds to concerns regarding online abuse and exploitation, whether or not it took place on the school premises or using school-owned equipment.
- 15.20. All concerns relating to online abuse and exploitation, including child sexual abuse and exploitation and criminal exploitation, are reported to the DSL and dealt with in line with the Child Protection and Safeguarding Policy.

Online hate

- 15.21. The school does not tolerate online hate content directed towards or posted by members of the school community.
- 15.22. Incidents of online hate are dealt with in line with the relevant school policy depending on the nature of the incident and those involved. e.g. Staff Code of Conduct and Handbook

Online radicalisation and extremism

- 15.23. The school's filtering system protects pupils and staff from viewing extremist content, and the monitoring system will alert members of staff to any trigger words typed into a computer
- 15.24. Concerns regarding a staff member or pupil being radicalised online are dealt with in line with the Child Protection and Safeguarding Policy and Prevent Duty Policy.

16. Remote learning

- 16.1. All staff and pupils using video communication must:
- Communicate in groups – one-to-one sessions are only carried out where necessary.
 - Wear suitable clothing – this includes others in their household.
 - Be situated in a suitable ‘public’ living area within the home with an appropriate background – ‘private’ living areas within the home, such as bedrooms, are not permitted during video communication.
 - Use appropriate language – this includes others in their household.
 - Maintain the standard of behaviour expected in school.
 - Use the necessary equipment and computer programs as intended.
 - Not record, store, or distribute video material without permission.
 - Ensure they have a stable connection to avoid disruption to lessons.
 - Always remain aware that they are visible.
- 16.2. All staff and pupils using audio communication must:
- Use appropriate language – this includes others in their household.
 - Maintain the standard of behaviour expected in school.
 - Use the necessary equipment and computer programs as intended.
 - Not record, store, or distribute audio material without permission.
 - Ensure they have a stable connection to avoid disruption to lessons.
 - Always remain aware that they can be heard.
- 16.3. The school will consider whether one-to-one sessions are appropriate in some circumstances, e.g. to provide support for pupils with SEND. This will be decided and approved by the SLT, in collaboration with the SENDCO.
- 16.4. Pupils not using devices or software as intended will be disciplined in line with the Behaviours Policy.
- 16.5. The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use.
- 16.6. The school will ensure that all school-owned equipment and technology used for remote learning has suitable anti-virus software installed, can establish

secure connections, can recover lost work, and allows for audio and visual material to be recorded or downloaded, where required.

- 16.7. The school will communicate to parents in writing about any precautionary measures that need to be put in place if their child is learning remotely using their own/family-owned equipment and technology, e.g. ensuring that their internet connection is secure.
- 16.8. During any period of remote learning, the school will maintain regular contact with parents to:
 - Reinforce the importance of children staying safe online.
 - Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.
 - Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
 - Direct parents to useful resources to help them keep their children safe online.
 - The school will not be responsible for providing access to the internet off the school premises and will not be responsible for providing online safety software, e.g. anti-virus software, on devices not owned by the school.

17. Monitoring and review

- 17.1. The school recognises that the online world is constantly changing; therefore, the DSL, ICT technicians and the headteacher conduct termly light-touch reviews of this policy to evaluate its effectiveness.
- 17.2. The governing body, headteacher and DSL review this policy in full on an annual basis and following any online safety incidents.
- 17.3. Any changes made to this policy are communicated to all members of the school community.

Appendix 1 – Online Safety Curriculum

At St Stephen's Primary School we follow government guidance for teaching online safety as contained in 'Teaching online safety in schools – Guidance supporting schools to teach their pupils how to stay safe online.' This guidance refers to the 'Education for a Connected World' framework for teaching, produced by the UK Internet Safety Council. There are eight aspects of Online Safety in this framework, as follows:



Self-image and identity

This strand explores the differences between online and offline identity beginning with self-awareness, shaping online identities and media influence in propagating stereotypes. It identifies effective routes for reporting and support and explores the impact of online technologies on self-image and behaviour.



Online relationships

This strand explores how technology shapes communication styles and identifies strategies for positive relationships in online communities. It offers opportunities to discuss relationships, respecting, giving and denying consent and behaviours that may lead to harm and how positive online interaction can empower and amplify voice.



Online reputation

This strand explores the concept of reputation and how others may use online information to make judgements. It offers opportunities to develop strategies to manage personal digital content effectively and capitalise on technology's capacity to create effective positive profiles.



Online bullying

This strand explores bullying and other online aggression and how technology impacts those issues. It offers strategies for effective reporting and intervention and considers how bullying and other aggressive behaviour relates to legislation.



Managing online information

This strand explores how online information is found, viewed and interpreted. It offers strategies for effective searching, critical evaluation of data, the recognition of risks and the management of online threats and challenges. It explores how online threats can pose risks to our physical safety as well as online safety. It also covers learning relevant to ethical publishing.



Health, well-being and lifestyle

This strand explores the impact that technology has on health, well-being and lifestyle e.g. mood, sleep, body health and relationships. It also includes understanding negative behaviours and issues amplified and sustained by online technologies and the strategies for dealing with them.



Privacy and security

This strand explores how personal online information can be used, stored, processed and shared. It offers both behavioural and technical strategies to limit impact on privacy and protect data and systems against compromise.



Copyright and ownership

This strand explores the concept of ownership of online content. It explores strategies for protecting personal content and crediting the rights of others as well as addressing potential consequences of illegal access, download and distribution.

We subscribe to National Online Safety, and use their teaching materials for most of our Online Safety teaching. This ensures coverage of the 'Education for a Connected World' framework.

Appendix 2: Online harms and risks – curriculum coverage

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	<p>Some online activities have age restrictions because they include content which is not appropriate for children under a specific age.</p> <p>Teaching includes the following:</p> <ul style="list-style-type: none"> • 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 	<p>This risk or harm is covered in the following curriculum area(s):</p> <ul style="list-style-type: none"> • Computing curriculum
How content can be used and shared	<p>Knowing what happens to information, comments or images that are put online.</p> <p>Teaching includes the following:</p> <ul style="list-style-type: none"> • 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) 	<p>This risk or harm is covered in the following curriculum area(s):</p> <ul style="list-style-type: none"> • PSHE • Computing curriculum
Disinformation, misinformation and hoaxes	<p>Some information shared online is accidentally or intentionally wrong, misleading or exaggerated.</p> <p>Teaching includes the following:</p>	<p>This risk or harm is covered in the following curriculum area(s):</p>

	<ul style="list-style-type: none"> • 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 • 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 	<ul style="list-style-type: none"> • Computing curriculum
Fake websites and scam emails	<p>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.</p> <p>Teaching includes the following:</p> <ul style="list-style-type: none"> • 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/groomed as a result of interacting with a fake website or scam email • Who pupils should go to for support 	<p>This risk or harm is covered in the following curriculum area(s):</p> <ul style="list-style-type: none"> • Computing curriculum
Online fraud	<p>Fraud can take place online and can have serious consequences for individuals and organisations.</p> <p>Teaching includes the following:</p> <ul style="list-style-type: none"> • 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 	<p>This risk or harm is covered in the following curriculum area(s):</p> <ul style="list-style-type: none"> • Computing curriculum
Password phishing	<p>Password phishing is the process by which people try to find out individuals' passwords so they can access protected content.</p> <p>Teaching includes the following:</p>	<p>This risk or harm is covered in the following curriculum area(s):</p>

	<ul style="list-style-type: none"> • 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 • 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 	<ul style="list-style-type: none"> • Computing curriculum
Personal data	<p>Online platforms and search engines gather personal data – this is often referred to as ‘harvesting’ or ‘farming’.</p> <p>Teaching includes the following:</p> <ul style="list-style-type: none"> • 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 	<p>This risk or harm is covered in the following curriculum area(s):</p> <ul style="list-style-type: none"> • Computing curriculum
Persuasive design	<p>Many devices, apps and games are designed to keep users online for longer than they might have planned or desired.</p> <p>Teaching includes the following:</p> <ul style="list-style-type: none"> • That the majority of games and platforms are designed to make money – their primary driver is to encourage people to stay online for as long as possible • How notifications are used to pull users back online 	<p>This risk or harm is covered in the following curriculum area(s):</p> <ul style="list-style-type: none"> • PSHE • Computing curriculum
Privacy settings	<p>Almost all devices, websites, apps and other online services come with privacy settings that can be used to control what is shared.</p> <p>Teaching includes the following:</p>	<p>This risk or harm is covered in the following curriculum area(s):</p>

	<ul style="list-style-type: none"> How to find information about privacy settings on various devices and platforms That privacy settings have limitations 	<ul style="list-style-type: none"> PSHE Computing curriculum
Targeting of online content	<p>Much of the information seen online is a result of some form of targeting.</p> <p>Teaching includes the following:</p> <ul style="list-style-type: none"> 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 	<p>This risk or harm is covered in the following curriculum area(s):</p> <ul style="list-style-type: none"> PSHE Computing curriculum
How to stay safe online		
Online abuse	<p>Some online behaviours are abusive. They are negative in nature, potentially harmful and, in some cases, can be illegal.</p> <p>Teaching includes the following:</p> <ul style="list-style-type: none"> 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 	<p>This risk or harm is covered in the following curriculum area(s):</p> <ul style="list-style-type: none"> PSHE Computing curriculum
Challenges	<p>Online challenges acquire mass followings and encourage others to take part in what they suggest.</p> <p>Teaching includes the following:</p> <ul style="list-style-type: none"> What an online challenge is and that, while some will be fun and harmless, others may be dangerous and even illegal 	<p>This risk or harm is covered in the following curriculum area(s):</p> <ul style="list-style-type: none"> PSHE Health education

	<ul style="list-style-type: none"> • 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 • The importance of telling an adult about challenges which include threats or secrecy – ‘chain letter’ style challenges 	
Fake profiles	<p>Not everyone online is who they say they are.</p> <p>Teaching includes the following:</p> <ul style="list-style-type: none"> • That, in some cases, profiles may be people posing as someone they are not or may be ‘bots’ • How to look out for fake profiles 	<p>This risk or harm is covered in the following curriculum area(s):</p> <ul style="list-style-type: none"> • PSHE • Computing curriculum
Grooming	<p>Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation (CSAE) and gangs (county lines).</p> <p>Teaching includes the following:</p> <ul style="list-style-type: none"> • 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 <p>At all stages, it is important to balance teaching pupils about making sensible decisions to stay safe whilst being clear it is never the fault of the child who is abused and why victim blaming is always wrong.</p>	<p>This risk or harm is covered in the following curriculum area(s):</p> <ul style="list-style-type: none"> • PSHE • Computing Curriculum
Live streaming	<p>Live streaming (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.</p> <p>Teaching includes the following:</p>	<p>This risk or harm is covered in the following curriculum area(s):</p> <ul style="list-style-type: none"> • PSHE

	<ul style="list-style-type: none"> • What the risks of carrying out live streaming are, e.g. the potential for people to record livestreams 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 • That 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 livestreamed, e.g. there is no way of knowing what will be shown next • The risks of grooming 	<ul style="list-style-type: none"> • Computing Curriculum
Unsafe communication	<p>Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met.</p> <p>Teaching includes the following:</p> <ul style="list-style-type: none"> • 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 	<p>This risk or harm is covered in the following curriculum area(s):</p> <ul style="list-style-type: none"> • PSHE • Computing curriculum
Wellbeing		
Impact on quality of life, physical and mental health and relationships	<p>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.</p> <p>Teaching includes the following:</p>	<p>This risk or harm is covered in the following curriculum area(s):</p>

	<ul style="list-style-type: none"> • 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 actually enjoying being online or just doing it out of habit due to peer pressure or the fear of missing out • That time spent online gives users less time to do other activities, which can lead some users to become physically inactive • 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 	<ul style="list-style-type: none"> • PSHE • Computing Curriculum
Online vs. offline behaviours	<p>People can often behave differently online to how they would act face to face.</p> <p>Teaching includes the following:</p> <ul style="list-style-type: none"> • 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/curated lives • How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face 	<p>This risk or harm is covered in the following curriculum area(s):</p> <ul style="list-style-type: none"> • PSHE • Computing Curriculum
Suicide, self-harm and eating disorders	<p>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 and should take care to avoid giving instructions or methods and avoid using language, videos and images.</p>	