

Online Safety Policy

Last updated: September 2024

To be reviewed: September 2025

Signed by:

Alison Halley	Headteacher	Date:	September 2021
Andrew York	Chair of governors	Date:	7th October 2021

Contents:

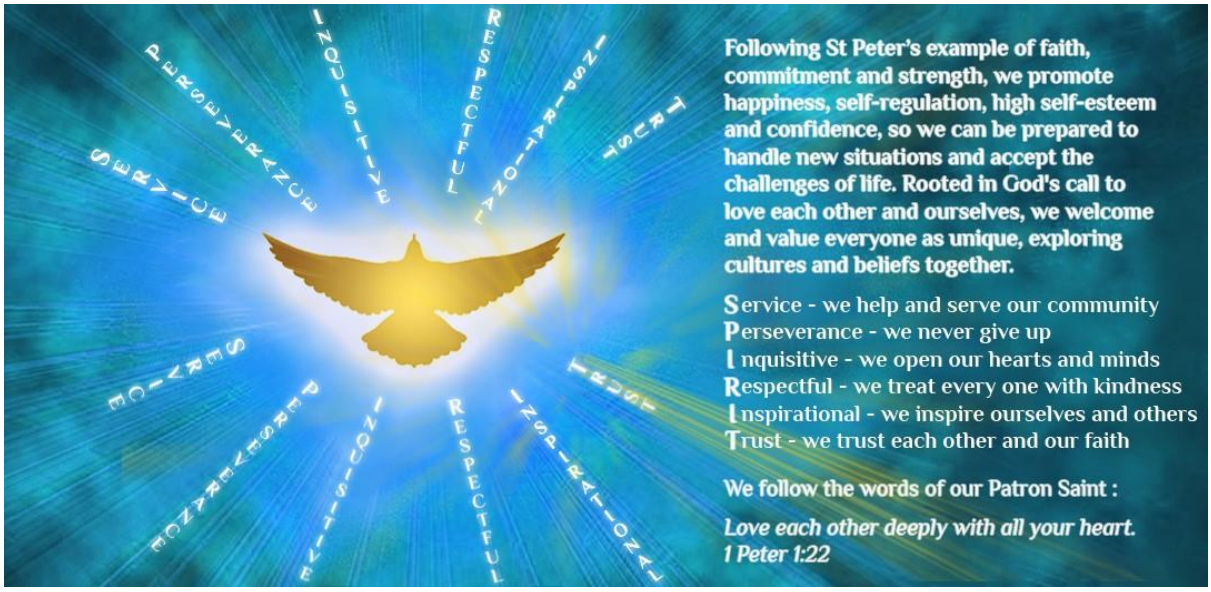
Statement of intent

1. Legal framework
2. Roles and responsibilities
3. The curriculum
4. Staff training
5. Educating parents
6. Classroom use
7. Internet access
8. Filtering and monitoring online activity
9. Network security
10. Emails
11. Social networking
12. Online hoaxes and harmful online challenges
13. The school website
14. Use of school-owned devices
15. Use of personal devices
16. Managing reports of online safety incidents
17. Responding to specific online safety concerns
18. Remote learning
19. Monitoring and review

Appendices

Appendix 1 – Online harms and risks – curriculum coverage

Our School SPIRIT



Intent

As a Church of England Primary school we are committed to a positive ethos and try to ensure that the whole school community reflect our Christian Vision and School SPIRIT. We instill Christian Values of mutual respect, forgiveness, kindness and love. We promote British Values. We believe in focusing on and rewarding good behaviour and respect for all.

Horbury St Peter's & Clifton CE Primary School 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 three 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 UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2021) 'Keeping children safe in education 2024'
- 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'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- National Cyber Security Centre (2018) 'Cyber Security: Small Business Guide'
- 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:

- Child Protection and Safeguarding Policy
- Anti-Bullying policy
- PSHE Policy
- RSHE Policy
- Staff Code of Conduct
- Behaviour Policy
- Data Protection Policy

2. Roles and responsibilities

2.1. The governing board 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 undergo safeguarding and child protection training, including online safety, at induction.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

2.2. The headteacher is responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSLs 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 DSLs and governing board to update this policy on an annual basis.
- Ensuring that the school filtering and monitoring systems are tested and reported on regularly.

2.3. The Computing Co-ordinators and Online Safety Leads are responsible for:

- Taking the lead responsibility for online safety in the school.
- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and ICT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.

- Ensuring safeguarding is considered in the school's approach to remote learning.
- Ensuring appropriate referrals are made to external agencies, as required.
- Keeping up-to-date with current research, legislation and online trends.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.
- Ensuring all members of the school community understand the reporting procedure.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the governing board about online safety as part of the safeguarding governor report on a termly basis.
- Working with the headteacher and governing board 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.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.

- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

2.6. Pupils are responsible for:

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

3. The curriculum

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

- RSE
- Physical health and wellbeing education
- PSHE
- Citizenship
- Computing

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.

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

3.4. Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum (links to Jigsaw, PHSE, RSE) and can 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

3.5. The online risks pupils may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in Appendix 1 of this policy.

3.6. The Online Safety Lead is involved with the development of the school's online safety curriculum.

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

3.8. 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?

3.9. External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The headteacher and Online Safety Lead decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

3.10. Before conducting a lesson or activity on online safety, the class teacher 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

Online Safety Lead is available to advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity.

3.11. 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 asking questions, and are not worried about getting into trouble or being judged.

3.12. 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 16 and 17 of this policy.

3.13. 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 16 and 17 of this policy.

4. Staff training

4.1. All staff receive safeguarding and child protection training, which includes online safety information, during their induction.

4.2. In addition to this training, staff also receive regular online safety updates as required and at least annually.

4.3. 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.

4.4. 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.

4.5. All staff receive a copy of this policy upon their induction and are informed of any changes to the policy.

4.6. Staff are required to adhere to the Staff Code of Conduct at all times, which includes provisions for the acceptable use of technologies and the use of social media.

4.7. All staff are informed about how to report online safety concerns, in line with sections 16 and 17 of this policy.

4.8. 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. Regular updates in regard to online safty appear in the school weekly Friday Flyer. Parents are also invited in bi annually to receive training in regard to the risks of online training.

5.2. Parents are provided with information about the school's approach to online safety and their role in protecting their children. The school sends out notifications which draw attention to website updates on the Keeping Children safe pages of the school website as well as the regular updates on the school weekly newsletter.

5.3. 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.

The school ensures that all of the above are regular features on our school Friday flyers and that our website also contains the latest information about this important online safety concerns.

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

5.5. Parental awareness regarding how they can support their children to be safe online is raised in the following ways:

- Parents' evenings
- Parent training sessions
- Newsletters
- Online resources

6. Classroom use

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

- Computers

- Laptops
- Tablets
- Internet
- Email
- Cameras
- Remote learning platforms

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

7. Internet access

7.1. Staff and other members of the school community can use school's internet network once they have read and understood the Acceptable Use Agreement.

8. Filtering and monitoring online activity

8.1. The ICT technician ensures the school's ICT network has appropriate filters and monitoring systems in place.

8.2. The headteacher and ICT technicians undertake a risk assessment to determine what filtering and monitoring systems are required. 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. ICT technicians undertake routine checks on the filtering and monitoring systems to ensure they are effective and appropriate.

8.3. Requests regarding making changes to the filtering system are directed to the Computing Co-ordinator and/ or ICT technician. Reports of inappropriate websites or materials are made to an ICT technician immediately, who investigates the matter and makes any necessary changes.

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

8.5. 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.

8.6. The school's network and school-owned devices are appropriately monitored.

8.7. All users of the network and school-owned devices are informed about how and why they are monitored.

8.8. Concerns identified through monitoring are reported to the DSL who manages the situation in line with sections 16 and 17 of this policy.

9. Network security

9.1. 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.

9.2. Staff and pupils are advised not to download unapproved software or open unfamiliar email attachments.

9.3. Staff members and pupils report all malware and virus attacks to ICT technicians.

9.4. All members of staff have their own unique usernames and private passwords to access the school's systems.

9.5. Pupils in school are provided with their own unique username.

9.6. Staff members and pupils are responsible for keeping their passwords private.

9.7. Users should not share their login details with others and are not allowed to log in as another user at any time.

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

9.9. Users inform ICT technicians if they forget their login details, who will arrange for the user to access the systems under different login details.

10. Emails

10.1. Access to and the use of emails is managed in line with the Data Protection Policy.

10.2. Staff and pupils are given approved school email accounts and are only able to use these accounts at school and when doing school-related work outside of school hours.

10.3. Any email that contains sensitive or personal information is only sent using secure and encrypted email.

10.4. Staff members and pupils are required to block spam and junk mail, and report the matter to ICT technicians. Chain letters, spam and all other emails from unknown sources are deleted without being opened. Pupils and staff are regularly trained on what phishing email and other malicious emails might look like and may include information on the following:

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

11. Social networking

Personal use

11.1. Access to social networking sites is filtered as appropriate.

11.2. Staff and pupils are not permitted to use social media for personal use during lesson time.

11.3. Staff should not use personal social media during break and lunchtimes; inappropriate or excessive use of personal social media during school hours may result in the removal of internet access or further action.

11.4. Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school.

11.5. 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.

11.6. Where staff have an existing personal relationship with a parent or pupil, and thus are connected with them on social media, e.g. they are close family friends with a parent at the school, they will ensure that their social media conduct relating to that parent is appropriate for their position in the school.

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

Use on behalf of the school

11.8. The use of social media on behalf of the school is conducted by the school's website manager.

11.9. The school's official social media channels are only used for official educational or engagement purposes.

11.10. Staff members must be authorised by the headteacher to access to the school's social media accounts.

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

11.12. The Staff Code of Conduct contains information on the acceptable use of social media – staff members are required to follow these expectations at all times.

12. Online hoaxes and harmful online challenges

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

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

12.3. Pupils are aware of who to report concerns to surrounding potentially harmful online challenges or hoaxes, e.g. by displaying posters. In our school this is their class teacher, who can then alert the DSLs.

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

12.5. The DSL will conduct a case-by-case assessment for any harmful online content brought to their attention, establishing the scale and nature of the possible risk to pupils, and whether the risk is one that is localised to the school or the local area, or whether it extends more widely across the country.

12.6. Where the harmful content is prevalent mainly in the local area, the DSL will consult with the LA about whether quick local action can prevent the hoax or challenge from spreading more widely.

12.7. The DSL will check the factual basis of harmful online challenges or hoaxes against a known, reliable and trustworthy source, e.g. the UK Safer Internet Centre, and will carefully consider if a challenge or story is a hoax or is harmful prior to providing any direct warnings to pupils or parents.

12.8. The school understands that discussing or naming a specific online hoax can, in some cases, needlessly increase pupils' exposure to distressing content, and will avoid showing pupils distressing content where doing so is not considered absolutely necessary for preventing its spread or easing fears amongst the school community.

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

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

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

- Factual and avoids 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 that is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.
- Age-appropriate and appropriate for the relevant pupils' developmental stage.
- Supportive.
- In line with section 16 and section 17 of this policy.

13. The school website

13.1. 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.

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

13.3. Personal information relating to staff and pupils is not published on the website.

14. Use of school-owned devices

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

- Laptop
- Tablet

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

14.3. Staff and pupils are not permitted to connect school-owned devices to public Wi-Fi networks.

14.4. All mobile school-owned devices are fitted with tracking software to ensure they can be retrieved if lost or stolen.

14.5. ICT technicians review all school-owned devices on a monthly basis to carry out software updates and ensure there is no inappropriate material or malware on the devices.

14.6. No software, apps or other programmes can be downloaded onto a device without authorisation from ICT technicians.

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

15. Use of personal devices (mobiles and other SMART Technology)

15.1. Any personal electronic device that is brought into school by staff is the responsibility of the user. They are not permitted to use their personal devices during lesson time, other than in an emergency.

15.2. Staff members are not permitted to use their personal devices to take photos or videos of pupils.

15.3. 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.

15.4. If a pupil needs to contact their parents during the school day, contact can be made via the staff in the school office.

15.5. Where a pupil uses accessibility features on a personal device to help them access education, e.g. where a pupil who is deaf uses their mobile phone to

adjust the settings on an internal hearing aid in response to audible stimuli during class, the arrangements and rules for conduct for this are developed and managed on a case-by-case basis.

15.6. The headteacher may authorise the use of mobile devices by a pupil for safety or precautionary use but it will be stored securely in the reception office

15.7. 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.

15.8. Any concerns about visitors' use of personal devices on the school premises are reported to the DSLs.

16. Managing reports of online safety incidents

16.1. Staff members and pupils are informed about what constitutes inappropriate online behaviour in the following ways:

- Staff training
- The online safety curriculum
- Assemblies

16.2. 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,

16.3. Concerns regarding a pupil's online behaviour are reported to the Online Safety Lead or DSL who investigates concerns with relevant staff members, e.g. the headteacher and ICT technicians.

16.4. Concerns regarding a pupil's online behaviour are dealt with in accordance with relevant policies depending on their nature, e.g. Behaviour Policy and Child Protection and Safeguarding Policy, or Peer to peer abuse or Cyberbullying policies.

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

16.6. 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.

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

16.8. Section 17 of this policy outlines how the school responds to specific online safety concerns, such as cyberbullying and peer-on-peer abuse.

17. Responding to specific online safety concerns

Cyberbullying

17.1. Cyberbullying, against either pupils or staff, is not tolerated.

17.2. Any incidents of cyberbullying are dealt with quickly and effectively whenever they occur.

17.3. 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 (peer-on-peer abuse)

17.4. The school recognises that peer-on-peer 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

17.5. The school responds to all concerns regarding online peer-on-peer abuse, whether or not the incident took place on the school premises or using school-owned equipment.

17.6. Concerns regarding online peer-on-peer abuse are reported to the DSL who will investigate the matter in line with the Child Protection and Safeguarding Policy and Peer to Peer Abuse Policies.

Upskirting

17.7. 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.

17.8. 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.

17.9. "Operating equipment" includes enabling, or securing, activation by another person without that person's knowledge, e.g. a motion activated camera.

17.10. Upskirting is not tolerated by the school.

17.11. 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 Safeguarding Policy.

Sexting and the sharing of indecent imagery of pupils

17.12. Sharing indecent 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.

17.13. Staff will receive appropriate training regarding child sexual development and will understand the difference between sexual behaviour that is considered normal and developmentally expected, and sexual behaviour that is inappropriate and/or harmful. Use of the Brooke Traffic Light system by DSLs will guide staff.

17.14. All concerns regarding sexting are reported to the DSL.

17.15. The DSLs will use their professional judgement, in line with the Safeguarding Policy, to determine whether the incident is experimental, i.e. expected for the developmental stage of the pupils involved, or aggravated, i.e. involves additional or abusive elements, the images are used recklessly or there is an intent to harm the pupil depicted.

17.16. Where the incident is categorised as 'experimental', the pupils involved are supported to understand the implications of sharing indecent imagery and to move forward from the incident.

17.17. Where there is reason to believe the incident will cause harm to the pupil depicted, or where the incident is classified as 'aggravated', 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

17.18. When investigating a report, staff members will not view and nude and semi-nude images unless there is a good and clear reason to do so.

17.19. If a staff member believes there is a good reason to view nude or semi-nude imagery as part of an investigation, they discuss this with the DSL and headteacher first.

17.20. The decision to view imagery is based on the professional judgement of the DSL and always complies with the Safeguarding Policy.

17.21. If a decision is made to view the imagery, the DSL will be satisfied that viewing:

- Is the only way to make a decision about whether to involve other agencies because it is not possible to establish the facts from any pupil involved.
- Is necessary in order to report the image to a website or suitable reporting agency to have the image taken down, or to support the pupil in taking down the image or in making a report.
- Is unavoidable because a pupil has presented it directly to a staff member or nudes or semi-nudes have been found on an education setting's device or network.

17.22. Where it is necessary to view the imagery the DSL will:

- Never copy, print, share, store or save images; this is illegal.
- Discuss the decision with the headteacher.
- Undertake the viewing themselves, or make sure viewing is undertaken by another member of the safeguarding team with delegated authority from the headteacher.
- Make sure viewing takes place with the headteacher or another member of the SLT in the room; additional people in the room will not view the imagery.
- Only view the imagery on the school premises.
- Ensure that, if devices need to be passed on to the police, the device is confiscated, disconnected from Wi-Fi and data and turned off immediately to avoid imagery being accessed remotely; the device will be secured until it can be collected by police.

17.23. Imagery will not be purposefully viewed where it will cause significant harm or distress to any pupil involved, in line with the DSL's professional judgement.

17.24. Any accidental or intentional viewing of imagery that is undertaken as part of an investigation is recorded.

17.25. Where a staff member has accidentally viewed a nude or semi-nude image, the DSL will ensure they are provided with the appropriate support, as viewing nude or semi-nude imagery of pupils can be distressing.

Online grooming, abuse and exploitation

17.26. Through the online safety curriculum, pupils are taught about how to recognise grooming and abuse and where they can go for support if they experience it.

17.27. The school responds to concerns regarding online grooming, abuse and exploitation, whether or not it took place on the school premises or using school-owned equipment.

17.28. All concerns relating to online grooming and exploitation, including child sexual abuse or exploitation (CSE) and child criminal exploitation (CCE), are reported to the DSL and dealt with in line with the Safeguarding Policy.

Online hate

17.29. The school does not tolerate online hate content directed towards or posted by members of the school community.

17.30. 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, Anti-Bullying Policy and Behaviour Policy.

Online radicalisation and extremism

17.31. The school's filtering system protects pupils and staff from viewing extremist content.

17.32. Concerns regarding a staff member or pupil being radicalised online are dealt with in line with the Safeguarding Policy and Prevent Duty Policy.

Mental health

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

17.33. Regular training will take place so that staff are aware that online activity in and outside school can have a substantial impact on a pupil's mental state both positively and negatively. The training will help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health.

18. Remote learning

18.1. 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.

18.2. 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.

18.3. 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 SENCO and Inclusion Leader.

18.4. Pupils not using devices or software as intended will be disciplined in line with the Behaviour Policy.

18.5. 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.

18.6. 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.

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

- Reinforce the importance of children staying safe online.

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

18.8. 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.

19. Monitoring and review

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

19.2. The next scheduled review date for this policy can be found on the front.

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

Safeguarding Leader (Including online Safety : Mrs Alison HALLEY. Other DSL's are Jenni Gallagher, Kay Barrett, Ruth Shepherd and Cath Rodgers – all help to ensure our Online safety is of the highest level.

Online Safety leaders who are also computing leads : Mrs Debbie Sadiq and Mrs Sue Stevens .

Appendix 1: 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	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 area(s): • Physical health and wellbeing education • Computing curriculum
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 area(s): • Relationships education • Computing curriculum
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 • Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons	This risk or harm is covered in the following curriculum area(s): • Relationships education and health education • Computing curriculum

	• 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/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 area(s): • Relationships education • Computing curriculum
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 area(s): • Relationships education • Computing curriculum
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	This risk or harm is covered in the following curriculum area(s): • Relationships education

	• 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	• Computing curriculum
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 area(s): • Relationships education • Computing curriculum
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 – 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 area(s): • Physical health and wellbeing education • Computing curriculum
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 area(s): • Relationships education

		• Computing curriculum
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 area(s): • Physical health and wellbeing education • Computing curriculum
How to stay safe online		
Online abuse	Some online behaviours are abusive. They are negative in nature, 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 area(s): • Relationships education • Physical health and wellbeing education • Computing curriculum
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	This risk or harm is covered in the following curriculum area(s): • Relationships education

	• 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	• Physical health and wellbeing education
Content which incites	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 area(s): • Relationships education • RSE
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 may be 'bots' • How to look out for fake profiles	This risk or harm is covered in the following curriculum area(s): • Relationships education • Computing curriculum
Grooming	Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation (CSAE) and gangs (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	This risk or harm is covered in the following curriculum area(s): • Relationships education • RSE

	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.	
Live streaming	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. Teaching includes the following: • 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	This risk or harm is covered in the following curriculum area(s): • Relationships education • Physical health and wellbeing education
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: • 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	This risk or harm is covered in the following curriculum area(s): • Relationships education • Computing curriculum

	• What online consent is and how to develop strategies to confidently say no to both friends and strangers online	
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 area(s): • Physical health and wellbeing education
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 actually enjoying being online or just doing it out of habit due to peer pressure or 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 • 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	This risk or harm is covered in the following curriculum area(s): • Physical health and wellbeing education

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/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 area(s): • Relationships education