ONLINE SAFETY POLICY

Abbey School

Version number	1.4	Date	November 2021
Approved by	Senior Leadership Team	Date	November 2021
Last reviewed on	November 2021		
Next review due by	November 2022		

Other relevant policies:

Safeguarding policy & procedures
Counter-bullying policy
Data protection policy and privacy notices
Acceptable use of ICT and internet policy
Behaviour policy
Allegations of Abuse Against Staff policy
Staff disciplinary policy and procedures
Staff code of conduct
PSHE policy & RSE policy
Remote Learning policy

Contents

1. Aims

Abbey 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 four areas of risk:

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

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

2. Legislation & guidance

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 2021'
- 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) 'Small Business Guide: Cyber Security'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Minimum Standards Residential Special School – NMSRSS - https://www.gov.uk/government/publications/residential-special-schools-national-minimum-standards

- Social Care Common Inspection framework – SCCIF- https://www.gov.uk/government/publications/social-care-common-inspection-framework-sccif-boarding-schools-and-residential-special-schools

3. Whole school approach to safe use of ICT

At Abbey School, creating a safe ICT learning environment includes three main elements:

- An effective range of technological tools
- Policies and procedures, with clear roles and responsibilities
- A comprehensive Online Safety education programme for pupils, staff and parents

4. Roles & Responsibilities

4.1. The Proprietor

The Proprietor is responsible for the school's safeguarding arrangements, which include online safety, with the support of the school Advisory Body. These responsibilities are operationally delegated to the Principal.

4.2. The Advisory Body

The Advisory 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 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.

4.3. The Principal

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

4.4. The DSL

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.
- 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 Advisory Body about online safety on a termly basis.

4.5. Head of IT

Head of IT is 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 principal.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

4.6. All Staff

All staff members are responsible for:

- Taking responsibility for the security of IT 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.

The school and all professionals will use their judgement when allowing pupils to have access to websites with streaming video applications and discuss the availability of these site to pupils with the Head of IT. The reasoning behind limits to these sites will be discussed with the pupils by staff members. When teaching SRE (Sex and Relationship Education) only approved resources, produced specifically for the purpose of education or prescribed by approved educational programmes, will be used.

It is acknowledged that this may restrict pupil independence or autonomy (for example by preventing pupils from accessing games sites that they may reach through a search engine without them first having been vetted by a staff member). However, pupil safety is paramount. Abbey School has pupils aged from 4-19 operating within a range of cognitive and developmental levels. As with all resources, a personalised approach is required in selecting the most appropriate resources to support a pupil in learning a particular skill. For this reason, all e-resources must be approved by the teacher using them as a resource before they are used for teaching, or before a pupil has access to them during their leisure time. This approval should occur before the teaching session without the pupil present.

Staff will ensure that pupils have:

- Safe use of e-mail
- Safe use of Internet including use of internet-based communication services
- Safe use of Internet including folders of YouTube videos that have been screened and approved by staff and no pupil access to YouTube search engines
- Safe (in some circumstances limited) access to websites that have streaming videos that come up at random and are not able to be previewed by staff beforehand
- Safe use of school network, equipment and data
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras

4.7. Pupils

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.

5. Managing online safety

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

The DSL has overall responsibility for the school's approach to online safety, with support from DDSLs where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online.

The importance of online safety is integrated across all school operations. These include, but are not limited to the following:

- Staff receive regular training and updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum (e.g. pupils are taught what to do if they see something that worries them online, to recognise what is ok / not ok online, how to report an issue – either online or to a trusted adult)
- Protections are in place such as appropriate filters to restrict potentially inappropriate online content
- Appropriate safety measures are in place to restrict online content e.g. setting up pupil folders containing content that has been screened by staff before viewing, use of search engines designed for children, e.g. Youtube Kids
- Risk assessments in place to establish appropriate levels of supervision and steps required to minimise other risks to pupils who are able to access internet independently
- Signposting parents to useful information about how to keep children safe online / providing parent training

6. Handling safety concerns

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

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

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, and manages concerns in accordance with relevant policies depending on their nature.

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

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

A record of online safety incidents is made using the Online Safety Incident Report Log. Where there is a safeguarding concern, procedures for reporting and recording concerns are followed in line with the school's Safeguarding Policy and Procedures.

7. Cyberbullying

Cyberbullying can include the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Menacing or upsetting responses to someone in a chatroom
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook

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

8. Peer-on-peer sexual abuse and harassment

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

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

- Threatening, facilitating or encouraging sexual violence
- Upskirting, i.e. taking a picture underneath a person's clothing without consent and with the intention of viewing their genitals, breasts or buttocks
- Sexualised online bullying, e.g. sexual jokes or taunts
- Unwanted and unsolicited sexual comments and messages
- Consensual or non-consensual sharing of sexualised imagery

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

The school responds to all concerns regarding online peer-on-peer sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online peer-on-peer abuse are reported to the DSL, who will investigate the matter in line with the Safeguarding Policy and Procedures.

9. Grooming and exploitation

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

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

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

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

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

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

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

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

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

Radicalisation

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

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

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

10. Mental Health

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

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. Concerns about the mental health of a pupil will be reported to the DSL and the Assistant Principal who is responsible for pupil welfare and wellbeing.

11. Cyber-crime

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

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

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

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

12. Online hoaxes and harmful online challenges

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

For the purposes of this policy, **"harmful online challenges"** refers to challenges that are targeted at young people and generally involve users recording themselves participating in an online challenge, distributing the video through social media channels and daring others to do the same. Although many

online challenges are harmless, an online challenge becomes harmful when it could potentially put the participant at risk of harm, either directly as a result of partaking in the challenge itself or indirectly as a result of the distribution of the video online – the latter will usually depend on the age of the pupil and the way in which they are depicted in the video.

Where staff suspect that a pupil may be involved in a harmful online challenge or online hoax, they will report this to the DSL immediately.

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

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

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

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

13. Online safety training for staff

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

14. Online safety and the curriculum

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

- RSE
- PSHE
- Computing

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

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using.

The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

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

The online risks pupils may face online are always considered when developing the curriculum. Appendix 1 outlines the key themes covered in online safety curriculum at each key stage. The school recognises that, while any pupil can be vulnerable online, pupils with SEND are particularly vulnerable and the curriculum is tailored so these pupils receive the information and support they need.

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

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

- Where does this organisation get their information from?
- What is their evidence base?
- Have they been externally quality assured?
- What is their background?
- Are they age-appropriate for pupils?
- Are they appropriate for pupils' developmental stage?

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

- Computers
- Laptops
- Tablets
- Email
- Cameras

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

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

If a staff member is concerned about anything pupils raise during online safety lessons and activities, or if a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Safeguarding Policy and Procedures.

15. Educating parents

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

Parental awareness regarding how they can support their children to be safe online is raised through newsletters or other communications home, through information via our website or parental engagement app (Weduc) and at termly reviews where relevant. 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.

- If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal (DSL) or in the Principal's absence, a deputy DSL.
- Concerns or queries about this policy can be raised with any member of staff or the Principal.

16. Internet access

Pupils (where able), staff and other members of the school community are only granted access to the school's internet network once they have read and signed the Acceptable Use Agreement.

A risk assessment is carried out by class teachers in order to establish the appropriate level of supervision for pupils accessing the Internet.

The residential element of Abbey School will allow students to access IT through a laptop, this internet access is monitored, logged and contented filtered based on the students' age. We have the following filtering levels in place. Web filtering will be category filtered appropriate to the age of the student.

- Under 13 Residential – Applied to accounts used by students under the age of 13
- Under 16 Residential – Applied to accounts used by students under the age of 16
- Under 19 Residential – Applied to accounts used by students under the age of 19

Students will not be allowed to connect their own devices to the school Wi-Fi.

Safe-guarding concerns around web browsing and use of IT will be raised with the appropriate safeguarding leads.

17. Filtering and monitoring online activity

The Head of IT ensures the school's ICT network has appropriate filters and monitoring systems in place, ensuring that 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The Head of IT undertakes 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. The Head of IT undertakes **monthly** checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system are directed to the Head of IT. Prior to making any changes to the filtering system, the Head of IT and the DSL conduct a risk assessment. Any changes made to the system are recorded by the Head of IT. Reports of inappropriate websites

or materials are made to the Head of IT and DSL immediately, who investigate the matter and makes any necessary changes.

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

The school's network and school-owned devices are appropriately monitored. All users of the network and school-owned devices are informed about how and why they are monitored. Concerns identified through monitoring are reported to the DSL who manages the situation in line with the Safeguarding Policy and Procedures.

18. Emails

Please refer to the Staff ICT and Internet Acceptable Use policy for guidance on social networking, staff use of emails.

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. Prior to being authorised to use the email system, staff and pupils (where able) must agree to the Acceptable Use Agreement.

19. Social networking

Personal use

Please refer to the Staff Code of Conduct and Staff ICT and Internet Acceptable Use policy for guidance on the use of social networking by staff.

Access to social networking sites is filtered as appropriate. Pupils are not permitted to use social media for personal use while in school.

Pupils are taught how to use social media safely and responsibly through the online safety curriculum.

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. Counter-Bullying Policy, Staff Code of Conduct and Behaviour Policy.

Use on behalf of the school

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

20. The school website

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

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

21. Use of devices

Please refer to the Staff Code of Conduct and Staff ICT and Internet Acceptable Use policy for guidance on staff use of devices.

Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g. tablets to use during lessons. Pupils are not permitted to bring in their own personal devices from home.

22. Remote learning

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

The school will consult with parents prior to the period of remote learning about what methods of delivering remote teaching are most suitable – alternate arrangements will be made where necessary.

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

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

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

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

23. Monitoring and review

This policy will be reviewed annually and any changes made to this policy are communicated to all members of the school community.

24. Appendix 1

All pupils will be taught about online safety as part of the PSHE and computing curriculum:

In **Key Stage 1**, pupils will be taught to:

- Use technology safely and respectfully, keeping personal information private
- Identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

In **Key Stage 2** pupils will be taught:

- To use technology safely, respectfully and responsibly
- To recognise acceptable and unacceptable behaviour
- To identify a range of ways to report concerns about content and contact

In **Key Stage 3**, pupils will be taught:

- To understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy
- To recognise inappropriate content, contact and conduct, and know how to report concerns

In **Key Stage 4** pupils will be taught:

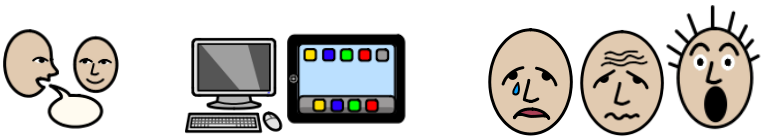
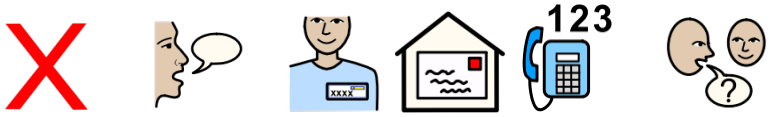
- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns

In **Key Stage 5** pupils will be taught:

- To recognise different forms of online gambling and the risks entailed, and to know where to go for help
- To recognise different forms of cyberbullying including those that take place through social media, and to know how to report concerns
- To recognise different ways that advertisers try to persuade us to spend money online

The safe use of social media and the internet will also be covered in other subjects where relevant.

25. Appendix 2: Acceptable use agreement for pupils

ACCEPTABLE USE OF THE SCHOOL'S ICT SYSTEMS AND INTERNET: AGREEMENT FOR PUPILS	
Name of pupil:	
When I use the school's ICT systems (computers or iPads) and get onto the internet in school I will: • Ask my teacher before I use ICT equipment  • Be kind to others when using ICT equipment  • Let my teacher know if I see something online that makes me upset, worried or scared  • Look after the school ICT equipment  • Never share my password with anyone, including my friends.  • Never give my personal information (my name, address, telephone numbers) to anyone without permission from my trusted adult 	
Signed (pupil):	**Date:**
Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will help my child to understands these.	
Signed (staff member):	**Date:**

26. Appendix 3: Online Safety Incident Log

ONLINE SAFETY INCIDENT LOG				
Date	**Where the incident took place**	**Description of the incident**	**Action taken**	**Name and signature of staff member recording the incident**

27. Appendix 4: Online Safety Risk Assessment Template

RISK ASSESSMENT – *ONLINE SAFETY*					
Name of assessor		Assessment date	Summer 2021	Nature of activity/risk assessed	Online Safety
Name of checker		Review date	Summer 2022	Persons at risk	Pupils

Related documents: Online Safety policy, Safeguarding children and young people in education policy, Countering Bullying policy, PSHE policy

Hazard or Activity	What might happen?	What risk controls are already in place?	Level of Risk			Are more controls or further action required? Details.	Residual Risk		
			L	S	DR		L	S	DR
Disclosure of personal data, e.g. name, address, location, contact details	Exposure to danger of harmful contact from strangers Grooming Stalking Cyberbullying Cyber crime Fraud	• Staff supporting when internet is being accessed • Strong filters installed on all school equipment • Only school equipment allowed to be connected to the internet by pupils (no personal devices may be brought in) • Pupils are helped to understand the risks of sharing information online through PSHE and computing lessons and what to do and how they can report any incidents				•			
Limited understanding of the dangers involved in accessing the internet	Exposure to harmful / inappropriate or illegal material or activities online Cyber crime Exploitation	• Staff supporting when internet is being accessed • Pupils taught about the risks associated with the Internet through the PSHE and computing curriculum • Strong filters installed on all school equipment • Information shared with parents about how to keep pupils safe online at home				•			

Inadvertently watching inappropriate content when accessing YouTube	Emotional harm or distress	• You Tube Kids used to safely access online content • Pupils supervised while online • Folders of pre-approved clips downloaded for older pupils to access • Pupils helped to understand what to do if they see something online that causes them distress through the PSHE curriculum				•			
Viewing inappropriate material online	Exposure to danger of harmful content e.g. pornography, suicide / self-harm ideology, violence Emotional harm or distress	• Staff supporting when internet is being accessed • Strong filters installed on all school equipment • Only school equipment allowed to be connected to the internet by pupils (no personal devices may be brought in) • Pupils are helped to recognise safe / unsafe material online through PSHE and computing lessons and what to do and how they can report any incidents				•			
Vulnerability to cyber-crime, e.g. scams and/or phishing	Cyber Crime Exploitation	• Strong filters installed on all school equipment • Pupils supervised while online				•			
Unsolicited contact from strangers	Agreeing to meet a stranger who they have met online Grooming for crime (inc. county lines) or sexual abuse Abuse Radicalisation Physical / emotional harm	• Pupils are helped to understand the risks of sharing information online or agreeing to meet someone they have met online through PSHE and computing lessons and what to do and how they can report any incidents • Pupils are helped to understand the concept of a 'stranger' through the PSHE curriculum using social stories and drama				•			

Online hoaxes and harmful online challenges	Physical injury / harm Emotional harm or distress	• Strong filters installed on all school equipment to ban apps / websites that commonly feature harmful online challenges or hoaxes, e.g. TikTok, Instagram • Staff made alert to new online challenges and hoaxes through e-bulletins and safeguarding updates				•			
Peer-on-peer sexual abuse and harassment e.g. sending / receiving sexual comments, messages or images	Abuse Exploitation Emotional harm / distress	• Pupils are helped to understand what can / can't be shared safely online and about healthy / unhealthy relationships through the PSHE curriculum using social stories and drama • Pupils taught what to do and how to report incidents				•			
Cyberbullying	Emotional harm / distress	• Pupils taught to recognise healthy and unhealthy relationships through the PSHE curriculum • Pupils taught what to do and how to report incidents				•			
Mental health affected as a result of online activity	Emotional harm / distress Eating disorders Low self-esteem, negative body image Self-harm	• Pupils taught through PSHE curriculum that not everything they see online is real • Pupils taught where to go for help if they are feeling unhappy or distressed • Staff alert to changes in pupil behaviour that might indicate mental health issues • Information shared with parents about the effect of online activity on mental health				•			

The risk assessment should be reviewed periodically and changed if it is no longer valid or if there are any significant changes to the hazards.

The findings of the risk assessment should be shared with everyone concerned.

TABLE A

Likelihood Score	Severity Score				
	1	2	3	4	5
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

Likelihood Score (L)	Hazard's Potential to be Realised
5	Very Likely
4	Likely
3	Fairly Likely
2	Unlikely
1	Very Unlikely

Severity Score (S)	Measure of outcome should the potential be realised
5	Catastrophic
4	Major
3	Moderate
2	Minor
1	Insignificant

TABLE B

Action Required	
Risk Level	**Level of Risk**
HIGH	Activity must be STOPPED. Suitable and sufficient risk control measures must be implemented before continuing the activity. Ideally alternative working practices should be used.
MEDIUM	Activity to proceed following prescribed safe system of work. Residual risks to be managed in safe system and recorded as such.
LOW	Level of risk satisfactory. Activity to proceed following prescribed safe system of work

TERMINOLOGY	
HAZARD	A Hazard is something that has the potential to cause harm (e.g. electricity, manual handling, slips & trips, strong acids)
DEGREE OF RISK (DR)	= **L**ikelihood x **S**everity
RESIDUAL RISK	The level of risk that remains after suitable control measures are introduced