



Together we make a difference!

Co-Head Teachers: Mr M Dodson & Mrs H Weston

Roe Farm Primary School

Online Safety Policy



Version Control				
No:	Date of Amendment:	Author:	Summary of Changes:	Date Shared with FGB:
1.0	February 2025	Helen Weston	Head teacher changed to Co-Heads	
2.0	February 2025	Helen Weston	Responsibilities amended and Senso alerting referenced. Pg 6/14: Links with PCSO Pg 10: Additional information added to Mental Health section Amended website responsibility.	

Approved By:	FGB
Date:	February 2025
Review Due Date:	12 Months

Contents:

Statement of intent

1. [Legal framework](#)
2. [Roles and responsibilities](#)
3. [Managing online safety](#)
4. [Cyberbullying](#)
5. [Child-on-child sexual abuse and harassment](#)
6. [Grooming and exploitation](#)
7. [Mental health](#)
8. [Online hoaxes and harmful online challenges](#)
9. [Cyber-crime](#)
10. [Online safety training for staff](#)
11. [Online safety and the curriculum](#)
12. [Use of technology in the classroom](#)
13. [Use of smart technology](#)
14. [Educating parents](#)
15. [Internet access](#)
16. [Filtering and monitoring online activity](#)
17. [Network security](#)
18. [Emails](#)
19. [Generative artificial intelligence \(AI\)](#)
20. [Social networking](#)
21. [The school website](#)
22. [Use of devices](#)
23. [Remote learning](#)
24. [Monitoring and review](#)

Appendix

- a. [Online harms and risks – curriculum coverage](#)

Statement of intent

Roe Farm 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 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.

1. Legal framework

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

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

This policy operates in conjunction with the following school policies:

- Social Media Policy
- Allegations of Abuse Against Staff Policy
- Technology Acceptable Use Agreement
- Cyber-security Policy
- Cyber Response and Recovery Plan
- Child Protection and Safeguarding Policy
- Child-on-child Abuse Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Behaviour Policy
- Disciplinary Policy and Procedure
- Data Protection Policy
- Confidentiality Policy
- Device User Agreement
- Prevent Duty Policy
- Remote Education Policy

2. Roles and responsibilities

The governing board will be responsible for:

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

The Co-Head Teachers will be responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Taking the lead responsibility for online safety in the school.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- Be responsible to monitoring and reviewing any 'Senso alerts' received and act accordingly.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Organising engagement with parents to keep them up-to-date with current online safety issues and how the school is keeping pupils safe.
- Working with the DSL and ICT technicians to conduct half-termly light-touch reviews of this policy.
- Working with the DSL and governing board to update this policy on an annual basis.

The DSL will be responsible for:

- 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.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the governing board about online safety on a termly basis.

- Working with the Co-Head Teachers and governing board to update this policy on an annual basis.

ICT technicians will be responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the Co-Head Teachers.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Working with the DSL and Co-Head Teachers to conduct half-termly light-touch reviews of this policy.

All staff members will be responsible for:

- Taking responsibility for the security of ICT systems and electronic data they use or have access to.
- Modelling good online behaviours.
- Maintaining a professional level of conduct in their personal use of technology.
- Having an awareness of online safety issues.
- Ensuring they are familiar with, and understand, the indicators that pupils may be unsafe online.
- Reporting concerns in line with the school's reporting procedure.
- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

Pupils will be responsible for:

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

3. Managing online safety

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

The Co-Head Teachers and Assistant Heads have overall responsibility for the school's approach to online safety, with support from the DSL and Deputy DSL where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL should liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

The importance of online safety is integrated across all school operations in the following ways:

- Staff and governors receive regular training
- Staff receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum

- Assemblies are conducted on the topic of remaining safe online and may be in response to issues that have arisen in school
- Links made with local PCSO, workshops delivered to classes/year groups

Handling online safety concerns

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

Staff will be aware that harmful online sexual behaviour can progress on a continuum, and appropriate and early intervention can prevent abusive behaviour in the future. Staff will also acknowledge that pupils displaying this type of behaviour are often victims of abuse themselves and should be suitably supported.

The victim of online harmful sexual behaviour may ask for no one to be told about the abuse. The DSL will consider whether sharing details of the abuse would put the victim in a more harmful position, or whether it is necessary in order to protect them from further harm. Ultimately the DSL will balance the victim's wishes against their duty to protect the victim and other young people. The DSL and other appropriate staff members will meet with the victim's parents to discuss the safeguarding measures that are being put in place to support their child and how the report will progress.

Confidentiality will not be promised, and information may be still shared lawfully, for example, if the DSL decides that there is a legal basis under UK GDPR such as the public task basis whereby it is in the public interest to share the information. If the decision is made to report abuse to children's social care or the police against the victim's wishes, this must be handled extremely carefully – the reasons for sharing the information should be explained to the victim and appropriate specialised support should be offered.

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

Concerns regarding a pupil's online behaviour are reported to the DSL, who investigates concerns with relevant staff members, e.g. the Co-Head Teachers and ICT technicians, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.

Where there is a concern that illegal activity has taken place, the Co-Head Teacher contacts the police.

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

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

4. Cyberbullying

Cyberbullying can include, but is not limited to, the following:

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras

- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

The school will be aware that certain pupils can be more at risk of abuse and/or bullying online, such as LGBTQ+ pupils and pupils with SEND.

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

5. Child-on-child sexual abuse and harassment

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

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

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

All staff will be aware of and promote a zero-tolerance approach to sexually harassing or abusive behaviour, and any attempts to pass such behaviour off as trivial or harmless. Staff will be aware that allowing such behaviour could lead to a school culture that normalises abuse and leads to pupils becoming less likely to report such conduct.

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

The school will be aware that interactions between the victim of online harmful sexual behaviour and the alleged perpetrator(s) are likely to occur over social media following the initial report, as well as interactions with other pupils taking "sides", often leading to repeat harassment. The school will respond to these incidents in line with the Child-on-child Abuse Policy and the Social Media Policy.

The school will respond to all concerns regarding online child-on-child sexual abuse and harassment, regardless of whether the incident took place on the school premises or using school-owned equipment. Concerns regarding online child-on-child abuse will be reported to the DSL, who will investigate the matter in line with the Child-on-child Abuse Policy and the Child Protection and Safeguarding Policy.

6. Grooming and exploitation

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

Staff will be aware that grooming often takes place online and that pupils who are being groomed are commonly unlikely to report this behaviour for many reasons, e.g. the pupil may have been manipulated into feeling a strong bond with their groomer and may have feelings of loyalty, admiration, or love, as well as fear, distress and confusion.

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The 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 online.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.
- Having money or new possessions, e.g. clothes and technological devices that they cannot or will not explain.

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

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

7. Mental health

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. The DSL will ensure that training is available to help ensure that staff members understand popular social media sites and terminology, the ways in which social media and the internet in general can impact mental health, and the indicators that a pupil is suffering from challenges in their mental health. Concerns about the mental health of a pupil will be dealt with in line with the Social, Emotional and Mental Health (SEMH) Policy.

Close links are made with external agencies and where relevant or needed appropriate referrals are made for example; Bridge the Gap for one: one support which may include Art/Music therapy, CAMHS. If a child has a social worker they are also updated and informed immediately so this can also be followed up.

8. Online hoaxes and harmful online challenges

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

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

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the 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 Co-Head Teachers 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, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or individual pupils at risk where appropriate.

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

9. 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 Co-Head Teachers will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

10. Online safety training for staff

The Co - head teachers will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

11. Online safety and the curriculum

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

- Relationships and health education
- PSHE
- Citizenship
- ICT

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

Pupils are taught the underpinning knowledge and behaviours that can help them to navigate the online world safely and confidently regardless of the device, platform or app they are using. The underpinning knowledge and behaviours pupils learn through the curriculum include the following:

- How to evaluate what they see online
- How to recognise techniques used for persuasion
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- Knowledge and behaviours that are covered in the government's online media literacy strategy

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 A](#) of this policy.

The DSL will be involved with the development of the school's online safety curriculum. Pupils will be consulted on the online safety curriculum, where appropriate, due to their unique knowledge of the kinds of websites they and their peers frequent and the kinds of behaviours in which they engage online.

Relevant members of staff, e.g. the SENCO and designated teacher for LAC, will work together to ensure the curriculum is tailored so that pupils who may be more vulnerable to online harms, e.g. pupils with SEND and LAC, receive the information and support they need.

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

Class teachers will review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of pupils.

External visitors may be invited into school to help with the delivery of certain aspects of the online safety curriculum. The Co-Head Teachers and DSL will decide when it is appropriate to invite external groups into school and ensure the visitors selected are appropriate.

Before conducting a lesson or activity on online safety, the class teacher and DSL will consider the topic that is being covered and the potential that pupils in the class have suffered or may be suffering from online abuse or harm in this way. The DSL will advise the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. Lessons and activities will be planned carefully so they do not draw attention to a pupil who is being or has been abused or harmed online, to avoid publicising the abuse.

During an online safety lesson or activity, the class teacher will ensure a safe environment is maintained in which pupils feel comfortable to say what they feel and ask questions, and are not worried about getting into trouble or being judged.

If a staff member is concerned about anything pupils raise during online safety lessons and activities, they will make a report in line with the Child Protection and Safeguarding Policy.

If a pupil makes a disclosure to a member of staff regarding online abuse following a lesson or activity, the staff member will follow the reporting procedure outlined in the Child Protection and Safeguarding Policy.

12. Use of technology in the classroom

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

- Laptops
- Ipads including use of camera
- Email

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that pupils use these platforms at home, the class teacher will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

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

13. Use of smart technology

While the school recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages.

Pupils will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the school's Technology Acceptable Use Agreement for Pupils.

The school recognises that pupils' unlimited and unrestricted access to the internet via mobile phone networks means that some pupils may use the internet in a way which breaches the school's acceptable use of ICT agreement for pupils.

Inappropriate use of smart technology may include:

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

Pupils will not be permitted to use smart devices or any other personal technology whilst in the classroom.

Where it is deemed necessary, the school will ban pupil's use of personal technology whilst on school site. All mobile phones are stored away during the day and returned to children prior to going home.

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

The school will hold assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner. These may be delivered by external visitors for example local PCSO.

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

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

14. Educating parents

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

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

- Child sexual abuse, including grooming.
- Exposure to radicalising content.
- Sharing of indecent imagery of pupils, e.g. sexting.
- Cyberbullying.
- Exposure to age-inappropriate content, e.g. pornography.
- Exposure to harmful content, e.g. content that encourages self-destructive behaviour.

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

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

- Use of Class Dojo to remind families
- Newsletters
- Online resources

15. Internet access

Pupils, staff and other members of the school community will only be granted access to the school's internet network once they have read and signed the Acceptable Use Agreement. A record will be kept of users who have been granted internet access in the school office.

All members of the school community will be encouraged to use the school's internet network, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

16. Filtering and monitoring online activity

The governing board will ensure the school's ICT network has appropriate filters and monitoring systems in place and that it is meeting the DfE's '[Filtering and monitoring standards for schools and colleges](#)'. The governing board will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

The co - head teachers will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs. Senso alerts will be regularly reviewed and monitored. Where relevant, these will be followed up and addressed.

The co - head teachers and ICT technicians will regularly review the filtering and monitoring systems. The filtering and monitoring systems the school implements will be appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks. ICT technicians will undertake monthly checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system will be directed to the co – head teachers. Prior to making any changes to the filtering system, ICT technicians and the DSL will conduct a risk assessment. Any changes made to the system will be recorded by ICT technicians. Reports of inappropriate websites or materials will be made to an ICT technician immediately, who will investigate the matter and makes any necessary changes.

Deliberate breaches of the filtering system will be 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 Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

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 will be appropriately monitored. All users of the network and school-owned devices will be informed about how and why they are monitored. Concerns identified through monitoring will be reported to the DSL who will manage the situation in line with the Child Protection and Safeguarding Policy.

17. Network security

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

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

All members of staff will have their own unique usernames and private passwords to access the school's systems. Pupils will be provided with their own unique username. Staff members will be responsible for keeping their passwords private. Passwords will have a minimum and maximum length and require a mixture of letters, numbers and symbols to ensure they are as secure as possible. Passwords will expire after 90 days, after which users will be required to change them.

Users will inform ICT technicians if they forget their login details, who will arrange for the user to access the systems under different login details. Users will not be permitted to share their login details with others and will not be allowed to log in as another user at any time. If a user is found to be sharing their login details or otherwise mistreating the password system, the Co-Head Teachers will be informed and will decide the necessary action to take.

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

18. Emails

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

Staff and pupils will be given approved school email accounts and will only be able to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff and pupils must agree to and sign the Acceptable Use Agreement. Personal email accounts will not be permitted to be used on the school site. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Staff members and pupils will be required to block spam and junk mail, and report the matter to ICT technicians. The school's monitoring system can detect inappropriate links, malware and profanity within emails – staff and pupils will be made aware of this. Chain letters, spam and all other emails from unknown sources will be deleted without being opened.

Any cyber-attacks initiated through emails will be managed in line with the Cyber Response and Recovery Plan.

19. Generative artificial intelligence (AI)

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

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

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

The school will take steps to ensure that personal and sensitive data is not entered into generative AI tools and that it is not identifiable.

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

20. The school website

The Business Manager/Assistant Head Teachers will be responsible for the overall content of the school website – they will ensure the content is appropriate, accurate, up-to-date and meets government requirements.

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

21. Use of devices

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

The use of personal devices on the school premises and for the purposes of school work will be managed in line with the Staff ICT and Electronic Devices Policy and Pupils' Personal Electronic Devices Policy.

22. Remote learning

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

23. Monitoring and review

The school recognises that the online world is constantly changing; therefore, the co - head teacher and ICT technician conduct half-termly light-touch reviews of this policy to evaluate its effectiveness.

The governing board, Co-Head Teachers and DSL will review this policy in full on an annual basis and following any online safety incidents.

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

Online harms and risks – curriculum coverage

[The table below contains information from the DfE's 'Teaching online safety in schools' guidance about what areas of online risk schools should teach pupils about. You can use this to assist your school in developing its own online safety curriculum; however, you must develop your curriculum in line with your local needs and the needs of your pupils.]

Teaching online safety in schools is a non-statutory guidance document (DfE, 2023) produced to help schools ensure that their pupils understand how to stay safe and behave online. It does not provide additional teaching requirements but rather 'brings together information that will help schools deliver online safety content within their curriculum and embed this within their wider whole school approach.

The guidance advises that schools refer to the Education for a connected world framework for age-specific advice about the online knowledge and skills that pupils should have the opportunity to develop at different stages of their lives. The tables below highlight where our computing curriculum aligns to this framework:

How to evaluate what they see online	
Covering this content will enable pupils to make judgements about what they see online and not automatically assume that what they see is true, valid or acceptable.	
Whether a website, URL or email is fake.	• Computing, Year 2, Online safety, Lesson 5: Is it true? • Computing, Year 3, Google: Computing systems and networks 2: Emailing, Lesson 5: Fake emails • Computing, Year 3, Microsoft: Computing systems and networks 2: Emailing, Lesson 5: Fake emails • Computing, Year 4, Online safety, Lesson 1: What happens when I search online?
What cookies do and what information they are sharing.	• Computing, Year 5, Online safety, Lesson 1: Online protection
If a person or organisation is who they say they are.	• Computing, Year 1, Online safety, Lesson 2: Online emotions • Computing, Year 6, Online safety, Lesson 1: Life online
Why a person wants them to see, send or believe something.	• Computing, Year 3, Online safety, Lesson 1: Beliefs, opinions and facts on the internet • Computing, Year 4, Online safety, Lesson 2: How do companies encourage us to buy online? • Computing, Year 6, Online safety, Lesson 3: Creating a positive online reputation • Computing, Year 6, Online safety, Lesson 6: Think before you click
Why a person wants their personal information.	• Computing, Year 3, Google: Computing systems and networks 2: Emailing, Lesson 5: Fake emails • Computing, Year 3, Microsoft: Computing systems and networks 2: Emailing, Lesson 5: Fake emails • Computing, Year 6, Online safety, Lesson 1: Life online

The reason why something has been posted.	• Computing, Year 4, Online safety, Lesson 2: How do companies encourage us to buy online? • Computing, Year 6, Online safety, Lesson 2: Sharing online
Whether something they see online is fact or opinion.	• Computing, Year 2, Online safety, Lesson 5: Is it true?

How to recognise techniques used for persuasion	
Covering this content will enable pupils to recognise the techniques that are often used to persuade or manipulate others.	
Online content which tries to make people believe something false is true or mislead (misinformation and disinformation)	• Computing, Year 2, Online safety, Lesson 5: Is it true? • Computing, Year 3, Google: Computing systems and networks 2: Emailing, Lesson 5: Fake emails • Computing, Year 3, Microsoft: Computing systems and networks 2: Emailing, Lesson 5: Fake emails • Computing, Year 3, Online safety, Lesson 1: Beliefs, opinions and facts on the internet • Computing, Year 4, Online safety, Lesson 1: What happens when I search online? • Computing, Year 4, Online safety, Lesson 3: Fact, opinion or belief?
Techniques that companies use to persuade people to buy something.	• Computing, Year 3, Online safety, Lesson 1: Beliefs, opinions and facts on the internet • Computing, Year 4, Online safety, Lesson 2: How do companies encourage us to buy online? • Computing, Year 5, Online safety, Lesson 1: Online protection
Ways in which criminals may try to defraud people online.	• Computing, Year 6, Online safety, Lesson 6: Think before you click
Ways to protect themselves from a range of cyber crimes.	• Computing, Year 2, Online safety, Lesson 4: It's my choice • Computing, Year 3, Google: Computing systems and networks 2: Emailing, Lesson 5: Fake emails • Computing, Year 3, Microsoft: Computing systems and networks 2: Emailing, Lesson 5: Fake emails

Online behaviour	
Covering this content will enable pupils to understand what acceptable and unacceptable online behaviour look like.	
That the same standard of behaviour and honesty apply on and offline, including the importance of respect for others	• Computing, Year 2, Online safety, Lesson 3: Who should I ask? • Computing, Year 3, Google: Computing systems and networks 2: Emailing, Lesson 4: Be kind online • Computing, Year 3, Microsoft: Computing systems and networks 2: Emailing, Lesson 4: Be kind online • Computing, Year 5, Online safety, Lesson 4: Online bullying • Computing, Year 6, Online safety, Lesson 2: Sharing online • Computing, Year 6, Online safety, Lesson 4: Capturing evidence
To recognise unacceptable behaviour in others	• Computing, Year 1, Online safety, Lesson 1: Using the internet safely • Computing, Year 1, Online safety, Lesson 2: Online emotions • Computing, Year 5, Online safety, Lesson 3: Online communication • Computing, Year 5, Online safety, Lesson 4: Online bullying • Computing, Year 6, Online safety, Lesson 1: Life online • Computing, Year 6, Online safety, Lesson 4: Capturing evidence
Looking at why people behave differently online, for example how anonymity (you do not know me) and invisibility (you cannot see me) affect what people do	• Computing, Year 5, Online safety, Lesson 3: Online communication • Computing, Year 5, Online safety, Lesson 4: Online bullying
Considering how to demonstrate empathy towards others (on and offline)	• Computing, Year 1, Online safety, Lesson 2: Online emotions • Computing, Year 1, Online safety, Lesson 3: Always be kind and considerate • Computing, Year 2, Online safety, Lesson 3: Who should I ask? • Computing, Year 5, Online safety, Lesson 4: Online bullying • Computing, Year 6, Online safety, Lesson 1: Life online • Computing, Year 6, Online safety, Lesson 4: Capturing evidence
Considering unacceptable online behaviours often passed off as so-called social norms or just banter, for example, negative	• Computing, Year 5, Online safety, Lesson 3: Online communication • Computing, Year 5, Online safety, Lesson 4: Online bullying

language being used as part of online gaming, but would never be tolerated offline	
--	--

How to identify online risks	
Covering this content will enable pupils to identify possible online risks and make informed decisions about how to act. This should not be about providing a list of what not to do online. The focus should be to help pupils assess a situation, think through the consequences of acting in different ways and decide on the best course of action.	
The ways in which someone may put themselves at risk online.	• Computing, Year 3, Online safety, Lesson 4: Rules of social media platforms • Computing, Year 6, Online safety, Lesson 1: Life online
Risks posed by another person's online behaviour.	• Computing, Year 2, Online safety, Lesson 3: Who should I ask? • Computing, Year 3, Google: Computing systems and networks 2: Emailing, Lesson 5: Fake emails • Computing, Year 3, Microsoft: Computing systems and networks 2: Emailing, Lesson 5: Fake emails • Computing, Year 5, Online safety, Lesson 4: Online bullying • Computing, Year 6, Online safety, Lesson 1: Life online • Computing, Year 6, Online safety, Lesson 2: Sharing online
When risk taking can be positive and negative.	• Computing, Year 6, Online safety, Lesson 1: Life online
Online reputation and the positive and negative aspects of an online digital footprint.	• Computing, Year 1, Online safety, Lesson 4: Posting and sharing on the internet • Computing, Year 6, Online safety, Lesson 3: Creating a positive online reputation
Sharing information online and how to make a judgement about when and how to share and who to share with.	• Computing, Year 1, Online safety, Lesson 1: Using the internet safely • Computing, Year 1, Online safety, Lesson 3: Always be kind and considerate • Computing, Year 2, Online safety, Lesson 3: Who should I ask? • Computing, Year 2, Online safety, Lesson 4: It's my choice • Computing, Year 3, Online safety, Lesson 4: Rules of social media platforms • Computing, Year 6, Online safety, Lesson 1: Life online
The risks of cyber crime, online fraud and identity theft.	• Computing, Year 6, Online safety, Lesson 6: Think before you click

How and when to seek support	
Covering this content will enable pupils to understand safe ways in which to seek support if they are concerned or upset by something they have seen online.	
Identify who trusted adults are.	• Computing, Year 1, Online safety, Lessons 1-3 • Computing, Year 2, Online safety, Lesson 4: It's my choice
Access support from the school, police, the National Crime Agency's Click CEOP reporting service for children and 3rd sector organisations such as Childline and Internet Watch Foundation.	• Computing, Year 3, Online safety, Lesson 2: When being online makes me upset • Computing, Year 5, Online safety, Lesson 5: Online health • Computing, Year 6, Online safety, Lesson 1: Life online
Report cyber crime, fraud and suspicious online activity, through organisations such as Action Fraud and the Advertising Standards Authority	• Computing, Year 6, Online safety, Lesson 6: Think before you click
Report inappropriate contact or content for various platforms and apps.	• Computing, Year 3, Online safety, Lesson 2: When being online makes me upset

Online media literacy strategy	
The online media literacy strategy sets out that the government will give internet users the knowledge and skills they need to make informed and safe choices online. It sets out 5 principles to underpin delivery of media literacy education.	
The risks of sharing personal data and how to protect their privacy.	• Computing, Year 1, Online safety, Lesson 1: Using the internet safely • Computing, Year 3, Online safety, Lesson 3: Sharing of information • Computing, Year 6, Online safety, Lesson 1: Life online • Computing, Year 6, Online safety, Lesson 6: Think before you click
How the online environment operates.	• Computing, Year 4, Online safety, Lesson 2: How do companies encourage us to buy online? • Computing, Year 6, Online safety, Lesson 6: Think before you click
How online content is generated and to critically analyse the content they consume.	• Computing, Year 4, Online safety, Lesson 1: What happens when I search online? • Computing, Year 4, Online safety, Lesson 2: How do companies encourage us to buy online?

That online actions can have offline consequences, and use this understanding in their online interactions.	• Computing, Year 2, Online safety, Lesson 1: What happens when I post online? • Computing, Year 2, Online safety, Lesson 3: Who should I ask? • Computing, Year 3, Google: Computing systems and networks 2: Emailing, Lesson 4: Be kind online • Computing, Year 5, Online safety, Lesson 3: Online communication • Computing, Year 5, Online safety, Lesson 4: Online bullying • Computing, Year 6, Online safety, Lesson 1: Life online • Computing, Year 6, Online safety, Lesson 2: Sharing online
How to participate positively in online engagement, while understanding the risks of engaging with others.	• Computing, Year 2, Online safety, Lesson 4: It's my choice • Computing, Year 5, Online safety, Lesson 3: Online communication • Computing, Year 5, Online safety, Lesson 4: Online bullying • Computing, Year 6, Online safety, Lesson 1: Life online

Age restrictions

Some online activities have age restrictions because they include content which is not appropriate for children under a specific age.

Explaining that age verification exists and why some sites require a user to verify their age, for example, online gambling and purchasing of certain age restricted materials such as alcohol.	• Computing, Year 3, Online safety, Lesson 4: Rules of social media platforms
Explaining why age restrictions exist, for example, they provide a warning that the site may contain disturbing material that is unsuitable for younger viewers.	• Computing, Year 3, Online safety, Lesson 4: Rules of social media platforms
Helping pupils understand how this content can be damaging to under-age consumers	• Computing, Year 3, Online safety, Lesson 4: Rules of social media platforms
Explaining what the age of digital consent means - the minimum age (13) at which	• Computing, Year 3, Online safety, Lesson 4: Rules of social media platforms

young people can agree to share information and sign up to social media without parental consent under General Data Protection Regulations.	
---	--

How content can be used and shared	
Knowing what happens to information, comments or images that are put online.	
What a digital footprint is, how it develops and how it can affect future prospects such as university and job applications.	• Computing, Year 1, Online safety, Lesson 4: Posting and sharing on the internet • Computing, Year 6, Online safety, Lesson 3: Creating a positive online reputation
How cookies work.	• Computing, Year 5, Online safety, Lesson 1: Online protection
How content can be shared, tagged and traced.	• Computing, Year 3, Online safety, Lesson 3: Sharing of information • Computing, Year 6, Online safety, Lesson 2: Sharing online
How difficult it is to remove something a user wishes they had not shared.	• Computing, Year 2, Online safety, Lesson 1: What happens when I post online? • Computing, Year 6, Online safety, Lesson 2: Sharing online
The risk of identity theft or targeted approach from fraudsters using information shared online.	• Computing, Year 6, Online safety, Lesson 6: Think before you click

Disinformation, misinformation, malinformation and hoaxes	
Some information shared online is accidentally or intentionally wrong, misleading, or exaggerated.	
Disinformation and why individuals or groups choose to share false information in order to deliberately deceive.	• Computing, Year 2, Online safety, Lesson 5: Is it true? • Computing, Year 3, Google: Computing systems and networks 2: Emailing, Lesson 5: Fake emails • Computing, Year 3, Microsoft: Computing systems and networks 2: Emailing, Lesson 5: Fake emails
Misinformation and being aware that false and misleading information can be shared inadvertently.	• Computing, Year 2, Online safety, Lesson 5: Is it true? • Computing, Year 3, Google: Computing systems and networks 2: Emailing, Lesson 5: Fake emails • Computing, Year 3, Microsoft: Computing systems and networks 2: Emailing, Lesson 5: Fake emails

Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons.	Computing, Year 2, Online safety, Lesson 5: Is it true?
How to measure and check authenticity online.	- Computing, Year 2, Online safety, Lesson 5: Is it true? - Computing, Year 3, Google: Computing systems and networks 2: Emailing, Lesson 5: Fake emails - Computing, Year 3, Microsoft: Computing systems and networks 2: Emailing, Lesson 5: Fake emails - Computing, Year 3, Online safety, Lesson 1: Beliefs, opinions and facts on the internet - Computing, Year 4, Online safety, Lesson 1: What happens when I search online? - Computing, Year 4, Online safety, Lesson 3: Fact, opinion or belief?
The potential consequences of sharing information that may not be true.	Computing, Year 2, Online safety, Lesson 5: Is it 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 another gain.	
How to look out for fake URLs and websites.	- Computing, Year 3, Online safety, Lesson 1: Beliefs, opinions and facts on the internet - Computing, Year 4, Online safety, Lesson 1: What happens when I search online?
Ensuring pupils understand what secure markings on websites are and how to assess the sources of emails.	- Computing, Year 3, Google: Computing systems and networks 2: Emailing, Lesson 5: Fake emails - Computing, Year 3, Microsoft: Computing systems and networks 2: Emailing, Lesson 5: Fake emails
Explaining the risks of entering information to a website which isn't secure.	- Computing, Year 3, Google: Computing systems and networks 2: Emailing, Lesson 5: Fake emails - Computing, Year 3, Microsoft: Computing systems and networks 2: Emailing, Lesson 5: Fake emails
What to do if harmed, targeted or groomed as a result of interacting with a fake website or scam email.	Computing, Year 3, Online safety, Lesson 2: When being online makes me upset
Who to go to and the range of support that is available.	Computing, Year 3, Online safety, Lesson 2: When being online makes me upset

Fraud (online)	
Fraud can take place online and can have serious consequences for individuals and organisations.	
What identity fraud, scams and phishing are.	• Computing, Year 3, Google: Computing systems and networks 2: Emailing, Lesson 5: Fake emails • Computing, Year 3, Microsoft: Computing systems and networks 2: Emailing, Lesson 5: Fake emails • Computing, Year 6, Online safety, Lesson 6: Think before you click
How to protect yourself and others against different types of online fraud.	• Computing, Year 6, Online safety, Lesson 6: Think before you click
The risk of sharing personal information that could be used by fraudsters.	• Computing, Year 3, Online safety, Lesson 3: Sharing of information
How to report fraud, phishing attempts, suspicious websites and adverts.	• Computing, Year 6, Online safety, Lesson 6: Think before you click

Password phishing	
Password phishing is the process by which people try to find out your passwords so they can access protected content.	
Why passwords are important, how to keep them safe and that others may try to trick you to reveal them.	• Computing, Year 3, Google: Computing systems and networks 2: Emailing, Lesson 2: Sending an email • Computing, Year 3, Microsoft: Computing systems and networks 2: Emailing, Lesson 2: Sending an email • Computing, Year 3, Online safety, Lesson 3: Sharing of information • Computing, Year 5, Online safety, Lesson 1: Online protection • Computing, Year 6, Online safety, Lesson 5: Password protection
Explaining how to recognise phishing scams, for example, those that try to get login credentials and passwords.	• Computing, Year 1, Online safety, Lesson 1: Using the internet safely
The importance of online security to protect against viruses (such as keylogging) that are designed to access, steal or copy passwords.	• Computing, Year 6, Online safety, Lesson 5: Password protection

What to do when a password is compromised or thought to be compromised.	Computing, Year 6, Online safety, Lesson 5: Password protection
---	---

Personal data	
Online platforms and search engines gather personal data. This is often referred to as 'harvesting' or 'farming'	
How cookies work.	Computing, Year 5, Online safety, Lesson 1: Online protection
How data is farmed from sources which look neutral, for example, websites that look like games or surveys that can gather lots of data about individuals.	Computing, Year 5, Online safety, Lesson 1: Online protection
How, and why, personal data is shared by online companies, for example, data being resold for targeted marketing by email and text (spam)	Computing, Year 5, Online safety, Lesson 1: Online protection
How pupils can protect themselves, including what to do if something goes wrong (for example data being hacked) and that acting quickly is essential	Computing, Year 1, Online safety, Lesson 1: Using the internet safely
The rights children have with regard to their data, including particular protections for children under the General Data Protection Regulations (GDPR).	Computing, Year 5, Online safety, Lesson 1: Online protection
How to limit the data companies can gather, including paying particular attention to boxes they tick when playing a game or accessing an app for the first time.	Computing, Year 5, Online safety, Lesson 1: Online protection

Persuasive design	
Many devices, apps and games are designed to keep users online for longer than they might have planned or desired.	
Explaining that the majority of games and platforms are businesses designed to make money - their primary driver is to encourage users to be online for as long as possible to encourage them to spend money (sometimes by offering incentives and offers) or generate advertising revenue	• Computing, Year 4, Online safety, Lesson 2: How do companies encourage us to buy online? • Computing, Year 5, Online safety, Lesson 1: Online protection

Privacy settings	
Almost all devices, websites, apps and other online services come with privacy setting that can be used to control what is shared.	
How to find information about privacy setting on various sites, apps, devices and platforms.	• Computing, Year 3, Online safety, Lesson 3: Sharing of information • Computing, Year 5, Online safety, Lesson 1: Online protection
Explaining that privacy settings have limitations, for example, they will not prevent someone posting something inappropriate.	• Computing, Year 3, Online safety, Lesson 3: Sharing of information

Targeting of online content	
Much of the information seen online is a result of some form of targeting.	
How adverts seen at the top of online searches and social media feeds have often come from companies paying to be on there and different people will see different adverts.	• Computing, Year 4, Online safety, Lesson 2: How do companies encourage us to buy online?
How the targeting is done, for example, software which monitors online behaviour (sites they have visited in the past, people who they are friends with) to target	• Computing, Year 4, Online safety, Lesson 2: How do companies encourage us to buy online?

advertises thought to be relevant to the individual user.	
The concept of clickbait and how companies can use it to draw people onto their sites and services.	• Computing, Year 4, Online safety, Lesson 2: How do companies encourage us to buy online?

Abuse (online)	
Some online behaviours are abusive. They are negative in nature, potentially harmful and in some cases can be illegal.	
Explaining about the types of online abuse including sexual, harassment, bullying, trolling and intimidation.	• Computing, Year 3, Google: Computing systems and networks 2: Emailing, Lesson 4: Be kind online • Computing, Year 3, Microsoft: Computing systems and networks 2: Emailing, Lesson 4: Be kind online
How to respond to online abuse including how to access help and support.	• Computing, Year 3, Online safety, Lesson 2: When being online makes me upset • Computing, Year 5, Online safety, Lesson 4: Online bullying • Computing, Year 6, Online safety, Lesson 4: Capturing evidence
How to respond when the abuse is anonymous.	• Computing, Year 3, Online safety, Lesson 2: When being online makes me upset • Computing, Year 5, Online safety, Lesson 3: Online communication • Computing, Year 5, Online safety, Lesson 4: Online bullying
Discussing the potential implications of online abuse, including the implications for victims.	• Computing, Year 5, Online safety, Lesson 4: Online bullying
Being clear about what good online behaviours do and don't look like.	• Computing, Year 5, Online safety, Lesson 3: Online communication • Computing, Year 5, Online safety, Lesson 4: Online bullying • Computing, Year 6, Online safety, Lesson 4: Capturing evidence

Challenges	
Online challenges acquire mass followings and encourage others to take part in what they suggest.	
Explaining what an online challenge is and that while some will be fun and harmless, others may be dangerous and or even illegal.	Computing, Year 6, Online safety, Lesson 1: Life online
Explaining to pupils that it is ok to say no and not take part.	Computing, Year 6, Online safety, Lesson 1: Life online
How and where to go for help if worried about a challenge.	Computing, Year 6, Online safety, Lesson 1: Life online

Fake profiles	
Not everyone online is who they say they are.	
Explaining that in some cases profiles may be people posing as someone they are not (such as an adult posing as a child) or may be bots (which are automated software programs designed to create and control fake social media accounts).	Computing, Year 4, Online safety, Lesson 4: What is a bot?
How to look out for fake profiles	Computing, Year 3, Online safety, Lesson 4: Rules of social media platforms

Unsafe communication	
Knowing different strategies for staying safe when communicating with others, especially people they do not know or have never met.	
Explaining that communicating safely online and protecting your privacy and data is important regardless of who you are communicating with.	- Computing, Year 3, Online safety, Lesson 4: Rules of social media platforms - Computing, Year 5, Online safety, Lesson 1: Online protection - Computing, Year 5, Online safety, Lesson 4: Online bullying - Computing, Year 6, Online safety, Lesson 1: Life online

Identifying indicators of risk and unsafe communications.	• Computing, Year 5, Online safety, Lesson 3: Online communication • Computing, Year 5, Online safety, Lesson 4: Online bullying • Computing, Year 6, Online safety, Lesson 1: Life online
Identifying risks associated with giving out addresses, phone numbers or email addresses to people you do not know or arranging to meet someone you have not met before.	• Computing, Year 6, Online safety, Lesson 1: Life online
Explaining about consent online and supporting pupils to develop strategies to confidently say “no” to both friends and strangers online.	• Computing, Year 2, Online safety, Lesson 3: Who should I ask? • Computing, Year 2, Online safety, Lesson 4: It's my choice • Computing, Year 6, Online safety, Lesson 1: Life online

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 on and offline.	
Helping pupils to evaluate critically what they are doing online, why they are doing it, and for how long (screen time).	• Computing, Year 4, Online safety, Lesson 5: What is my #TechTimetable like?
Helping pupils to consider quality versus quantity of online activity	• Computing, Year 5, Online safety, Lesson 5: Online health
Explaining that pupils need to consider if they are actually enjoying being online or just doing it out of habit, due to peer pressure or the fear of missing out	• Computing, Year 4, Online safety, Lesson 5: What is my #TechTimetable like?
Helping pupils to understand that time spent online gives users less time to do other activities - this can lead to some users becoming physically inactive.	• Computing, Year 4, Online safety, Lesson 5: What is my #TechTimetable like? • Computing, Year 5, Online safety, Lesson 5: Online health
Exploring the impact that excessive social media usage can have on levels of	• Computing, Year 5, Online safety, Lesson 5: Online health

anxiety, depression and other mental health issues.	
Explaining that isolation and loneliness can affect pupils and that it is very important for pupils to discuss their feeling with an adult and seek support.	Computing, Year 5, Online safety, Lesson 5: Online health
Where to get help.	Computing, Year 5, Online safety, Lesson 5: Online health
Online versus offline behaviours and reputational damage	
People can behave differently online to how they would act face to face.	
Discussing how and why people are unkind or hurtful online, when they would not necessarily be unkind to someone face to face.	Computing, Year 5, Online safety, Lesson 4: Online bullying
Looking at strategies for positive use.	Computing, Year 6, Online safety, Lesson 3: Creating a positive online reputation