E-Safety Policy

Contents:

1. Statement of Intent

Furze Platt Senior School understands that using online services is an important aspect of raising educational standards, promoting student 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 students and staff.

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

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

The measures implemented to protect students 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 students and staff.

2. Legal Framework

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

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

2.2. This policy will be used in conjunction with the following school policies and procedures:

- Anti-Bullying Policy
- Cyber-bullying Policy
- Child Protection & Safeguarding Policy
- Data Protection Policy
- Relationships & Sex Education Policy
- Behaviour Policy
- Social Media Policy
- Acceptable ICT Use Agreement

For the purposes of this policy, 'mobile devices' shall be defined as a portable computing device such as a smartphone or tablet computer.

3. Roles & Responsibilities

3.1. The governing body is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy every two years.
- 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.

3.2. The Headteacher is responsible for:

- Supporting the DSL and any deputies by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all students 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 students safe.

3.3. The DSL is responsible for:

- Taking the lead responsibility for online safety in the school.
- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that students with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the Assistant Headteacher (Inclusion) and IT Strategy Manager.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring appropriate referrals are made to external agencies, as required.
- Staying up-to-date with current research, legislation and online trends.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by students and staff.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision, and using this data to update the school's procedures.
- Reporting to the governing board about online safety as required, at least annually.
- Working with the IT Strategy Manager to review this policy on an ongoing basis.
- Working closely with the police during police investigations.
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- 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 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.
- Reporting to Governors on filtering and monitoring systems.

3.4. IT Strategy Manager 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 DSL.
- Ensuring that the school's filtering and monitoring systems are updated as

appropriate.
- Working with the DSL to monitor this policy on an ongoing basis.

3.5. 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.
- 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.

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

4. The Curriculum

4.1. Online safety is embedded throughout the curriculum; however, it is particularly addressed in the following subjects:
- PSHE / Citizenship (including RSE)
- Computing / ICT

4.2. Aspects of eSafety are covered across all year groups:
- Year 7-9 – How to be safe online and cybercrime.
- Year 7 – Relationships Education - Online bullying and online safety / Using Computers Safely (Social Media, Keeping data safe and searching the internet)
- Year 8 – Mental wellbeing – keeping mentally healthy online / Computer Crime and Cyber Security (Emails scams, cyber-attacks and Computer crime)
- Year 9 – RSE – pornography, sexting and sharing images
- Year 10 – Social media and 'selfie safety'
- Year 10 and 11 Safety from online scams and safe use of online profiles
- Year 11 - Education around sharing of images and also revenge pornography
- Year 10 and12 – DASH charity – law around sharing of images

4.3. The curriculum and the school's approach to online safety is developed in line with the UK Council for Child Internet Safety's 'Education for a Connected World' framework, the DfE's 'Teaching online safety in school' guidance and other reputable sources.

4.4. Students 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.

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

4.6. The underpinning knowledge and behaviours students 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

4.7. The online risks students may face online are always considered when developing the curriculum.

4.8. The DSL is involved with the development of the school's online safety curriculum.

4.9. The school recognises that, while any student can be vulnerable online, there are some students who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. students with SEND and Looked After Children. Relevant members of staff, e.g. the SENCO and designated teacher for Looked After

Children, work together to ensure the curriculum is tailored so these students receive the information and support they need.

4.10. Class teachers review external resources prior to using them for the online safety curriculum, to ensure they are appropriate for the cohort of students. 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 students?
- Are they appropriate for students' developmental stage?

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

4.12. Before conducting a lesson or activity on online safety, the class teacher and DSL consider the topic that is being covered and the potential that students in the class have suffered or may be suffering from online abuse or harm in this way. The DSL advises the staff member on how to best support any student who may be especially impacted by a lesson or activity.

4.13. Lessons and activities are planned carefully so they do not draw attention to a student who is being or has been abused or harmed online, to avoid publicising the abuse.

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

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

4.16. If a student 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 school's Child Protection & Safeguarding Policy.

5. Staff Training

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

5.2. Online safety training for staff is updated annually and is delivered in line with advice from the three local safeguarding partners.

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

5.4. The DSL undergoes training to provide them with the knowledge and skills they need to carry out their role, this includes online safety training. This training is updated at least every two years.

5.5. In addition to this formal training, the DSL and any deputies receive regular online safety updates to allow them to keep up with any developments relevant to their role. In relation to online safety, these updates allow the DSL and their deputies to:

- Understand the unique risks associated with online safety and be confident that they have the relevant knowledge and capability required to keep students safe while they are online at school.
- Recognise the additional risks that students with SEND face online and offer them support to stay safe online.

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

6. Educating Parents

6.1. The school works in partnership with parents to ensure students stay safe online at school and at home.

6.2. Parents are provided with information about the school's approach to online safety and their role in protecting their children. Parental awareness is raised in the following ways:

- Parents' information evenings
- Newsletters
- School website
- furzeplatt.onlinesafetyhub.uk

7. Classroom Use

7.1. Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that students use these platforms at home, the class teacher always reviews and evaluates the resource.

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

7.3. Filtering and monitoring systems are used to monitor students use of online materials.

8. Internet Access

Educating students:

8.1. All students of the school community are encouraged to use the school's network instead of mobile data, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

9. 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 deputies and the Headteacher where appropriate, and will ensure that there are strong processes in place to handle any concerns about pupils' safety online. The DSL will liaise with the police or children's social care services for support responding to harmful online sexual behaviour.

10. Filtering and Monitoring Online Activity

10.1. The DSL and IT Strategy Manager ensure the school's IT network has appropriate filters and monitoring systems in place.

10.2. The DSL and IT Strategy Manager undertake a annual audit to assess risk and determine what filtering and monitoring systems are required.

10.3. The filtering and monitoring systems the school implements are appropriate to students' ages, the number of students using the network, how often students access the network, and the proportionality of costs compared to the risks.

10.4. The DSL and IT Strategy Manager ensure 'over blocking' does not lead to unreasonable restrictions as to what students can be taught with regards to online teaching and safeguarding.

10.5. The IT Strategy Manager undertakes regular checks on the filtering and monitoring systems to ensure they are effective and appropriate.

10.6. Requests regarding changes to the filtering system are directed to the IT Strategy Manage who, working with the DSL, will make a decision. Any changes made to the system are recorded by the IT Support Team.

10.7. Reports of inappropriate websites or materials are made to the IT Strategy Manager immediately, who investigate the matter and makes any necessary changes.

10.8. 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.

10.9. The school's network and school-owned devices are appropriately monitored. The school retains the right to monitor all IT usage, and where any breaches of school policy are identified they will be dealt with in line with the Disciplinary Policy.
10.10. All users of the network and school-owned devices are informed about how and why they are monitored. This is in the acceptable usage guidance which is shared with students when they join the school.
10.11. Concerns identified through monitoring are reported to the DSL who manages the situation in line with the school's Child Protection & Safeguarding Policy.
10.12. School staff will report any concerns around online activity via the schools safeguarding reporting systems. These incidents can then be tracked, monitored and outcomes recorded.

11. Artificial Intelligence

11.1 Filtering and monitoring are used to support online safety when using EduTech systems. AI is now a significant part of pupils' digital experience and the relevant risk including deepfakes, misinformation and disinformation and harmful content should be monitored.
11.2 It is also important that staff and students recognise the associated risks of imputing personal data into AI tools.
11.3 When considering the use of EduTech platforms, the IT Manager and DSL will consider any potential risks in line with the Department for Educations Generative AI: product safety standards (2026)

12. Network Security

Personal Use:
11.1. Technical security features, such as anti-virus software, are kept up-to-date and managed by the IT Strategy Manager.
11.2. Appropriate firewalls are switched on at all times.
11.3. The IT Strategy Manager monitors the firewalls, filtering and monitoring on a regular basis to ensure they are running correctly, and to carry out any required updates.
11.4. Staff members and students are required to report all malware and virus attacks to the IT Support Team.
11.5. All members of staff and students have their own unique usernames and passwords to access the school's systems.
11.6. Users are not permitted to share their login details with others and are not permitted to use another person's account at any time.
11.7. Users are required to lock access to devices and systems when they are not in use.
11.8. Students who forget their login details should inform their class teacher, who will be able to reset them. Staff members should contact the IT Support Team who will assist.
11.9. If a user is found to be sharing their login details or otherwise mistreating the password system, the IT Strategy Manager is informed and decides the necessary action to take.

13. Social Networking

12.1. Access to social networking sites is filtered as appropriate.
12.2. Students in Year 7-11 are not permitted to use social media for personal use during lesson time.
12.3. Staff and Sixth Formers can use personal social media while not in lessons.
12.4. Staff members are advised that their conduct on social media can have an impact on their role and reputation within the school.
12.5. Staff receive annual training on how to use social media safely and responsibly.
12.6. Staff are not permitted to communicate with students or parents over personal social networking sites and are reminded to alter their privacy settings to ensure students and parents are not able to contact them on social media.
12.7. Students are taught how to use social media safely and responsibly through the online safety curriculum.
12.8. 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.

Use on behalf of the school:

12.9. The use of social media on behalf of the school is conducted in line with the Social Media Policy.

14. The School Website

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

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

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

13.4. Images and videos are only posted on the website if the required photography usage permissions have been met.

15. Responding to Specific Online Safety Concerns

14.1. Details of how the school responds to specific online safety concerns can be found in the Child Protection and Safeguarding Policy.

16. Remote learning

15.1. The school will risk assess the technology used for remote learning prior to use and ensure that there are no privacy issues or scope for inappropriate use.

15.2. While periods of remote learning cannot always be forewarned, the school will endeavor to ensure students are able to access their curriculum from home.

15.3. 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.

15.4. 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.

15.5. 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 students' devices.

17. Monitoring & Review

16.1. The school recognises that the online world is constantly changing; therefore, the DSL and IT Strategy Manager regularly review this policy to evaluate its effectiveness.

16.2. Senior Leadership Team and the Pupils & Parents Committee will evaluate and review this E-Safety Policy every two years, taking into account the latest developments in ICT and the feedback from staff/students.

The policy will be reviewed immediately in the event of any online safety incidents.

APPENDIX 1 - 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.

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

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

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

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

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

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

	• How to identify indicators of risk and unsafe communications • The risks associated with giving out addresses, phone numbers or email addresses to people pupils do not know, or arranging to meet someone they have not met before • What online consent is and how to develop strategies to confidently say no to both friends and strangers online	• Computing curriculum
Wellbeing		
Impact on confidence (including body confidence)	Knowing about the impact of comparisons to 'unrealistic' online images. Teaching includes the following: • The issue of using image filters and digital enhancement • The role of social media influencers, including that they are paid to influence the behaviour of their followers • The issue of photo manipulation, including why people do it and how to look out for it	This risk or harm is covered in the following curriculum area(s): • Health education
Impact on quality of life, physical and mental health and relationships	Knowing how to identify when online behaviours stop being fun and begin to create anxiety, including that there needs to be a balance between time spent online and offline. Teaching includes the following: • How to evaluate critically what pupils are doing online, why they are doing it and for how long (screen time) • How to consider quality vs. quantity of online activity • The need for pupils to consider if they are actually enjoying being online or just doing it out of habit due to peer pressure or the fear or missing out • That time spent online gives users less time to do other activities, which can lead some users to become physically inactive • The impact that excessive social media usage can have on levels of anxiety, depression and other mental health issues • That isolation and loneliness can affect pupils and that it is very important for them to discuss their feelings with an adult and seek support • Where to get help	This risk or harm is covered in the following curriculum area(s): • Health education

Online vs. offline behaviours	People can often behave differently online to how they would act face to face. Teaching includes the following: • How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressures around having perfect/curated lives • How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face	This risk or harm is covered in the following curriculum area(s): • Relationships education
Reputational damage	What users post can affect future career opportunities and relationships – both positively and negatively. Teaching includes the following: • Strategies for positive use • How to build a professional online profile	This risk or harm is covered in the following curriculum area(s): • RSE
Suicide, self-harm and eating disorders	Pupils may raise topics including eating disorders, self-harm and suicide. Teachers must be aware of the risks of encouraging or making these seem a more viable option for pupils and should take care to avoid giving instructions or methods and avoid using language, videos and images.	