Online Safety Policy

Contents:

Statement of intent

1. Legal framework
2. Roles and responsibilities
3. Managing online safety
4. Online safety training for staff
5. Use of technology in the classroom
6. Staff use of internet and Technology
7. Educating parents
8. Internet access
9. Filtering and monitoring online activity
10. Network security
11. Emails
12. Social networking
13. The school website
14. Monitoring and review

Appendix

a. Online harms and risks – curriculum coverage

Statement of intent

Oakleigh 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. At Oakleigh School we recognise that due to the complex needs of the pupils, it is highly unlikely that our pupils are likely to access or

browse the internet independently or to take part in or be the victims of cyber-bullying. We need to ensure that staff are confident to use online material safely and know when and how to report any

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 (2024) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2025) 'Keeping children safe in education 2025'
- DfE (2023) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- DfE (2023) 'Generative artificial intelligence in education'
- Department for Science, Innovation and Technology and UK Council for Internet Safety (2024) '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:

- Use of Social Media Policy
- Allegations of Abuse Against Staff Policy
- Child Protection and Safeguarding Policy
- Staff Code of Conduct
- Behaviour Policy
- Disciplinary Policy and Procedure
- Data Protection Policy
- Staff ICT and Electronic Devices Policy
- Prevent Duty Policy

2. Roles and responsibilities

The Governing body 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 Headteacher 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.
- Supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- 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.

ICT technicians (Interm UK until March 2026, From April 2026- it will be 28 Degrees IT) will be responsible for:

- Providing technical support to ensure working use of safeguarding software and firewall.
- Implementing appropriate security measures as directed by the Headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- The DSL and Headteacher will meet to discuss any IT issues within this Policy annually

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.
- Reporting concerns in line with the school's reporting procedure.

Reviewed by Emily Wharton January 2026/Approved by FGB 2.2.26
To be reviewed January 2027

- Where relevant to their role, ensuring online safety is embedded in their teaching of the curriculum.

3. Managing online safety

All staff will be aware that technology is a significant component in many safeguarding and wellbeing issues affecting young people. Due to the complex needs of the pupils it is the staff duty to ensure all staff are ensuring all internet and device used by the children is safe and had no harmful content

The DSL has overall responsibility for the school's approach to online safety, with support from deputies and the Headteacher where appropriate.

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

4. Online safety training for staff

The DSL will ensure that all safeguarding training given to staff includes elements of online safety, including how the internet can facilitate abuse and exploitation, and understanding the expectations, roles and responsibilities relating to filtering and monitoring systems. Oakleigh school will ensure all staff understand how to report any concerns when using online materials with pupils

5. Use of technology in the classroom

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

- Computers
- Laptops
- Communication Devices
- Ipads

Prior to using any websites, tools, apps or other online platforms in the classroom, or recommending that parents may 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.

6. Staff – Use of Internet & Technology

- Staff can access the Internet for personal use in their free time (coffee breaks, lunchtime and before or after school), not with the children in the classroom. Staff will need to use the Wi-Fi Guest login posted up in the staffroom for mobile devices.
- School laptops/tablets or personal mobile devices should not be used to view any internet sites that display pornographic, racist, illegal, discriminatory or any other offensive material, or any material that common-sense dictates is inappropriate for viewing in a school. This still applies when using a laptop offsite. If this happens accidentally, please inform a member of the senior leadership team. The school reserves the right to monitor any Internet sites visited, or any internet use and inappropriate use may result in disciplinary proceedings.
- Smart devices such as Apple Watches and Fitbits – If the device has an airplane mode, this should be enabled when working with children. Text notifications on all devices should be disabled.
- Risk from viruses means that staff must be very careful about downloading software, or opening attachments on e-mails from unknown senders. If in doubt, consult the ICT Co-ordinator/Manager. If you open an attachment from an unreliable source, please inform the ICT Co-ordinator/Manager.
- All school systems are protected by up-to-date virus software and by the London Grid for Learning, which is our Internet service provider, and has a filter designed to restrict access to inappropriate websites, including filtering of YouTube. In practice this can sometimes prevent access to perfectly OK sites. If you need help with unblocking sites, please contact the ICT co-ordinator/Manager.
- In the event that illegal material, or material that is, or is suspected to be, a child sexual abuse image, is found on the school's network, or evidence suggests that illegal material has been accessed, the police will be contacted.

Staff – Use of Social Media

- Information of any kind about school or colleagues should not be shared via email or social networking sites such as Facebook or X etc. Care should be taken in text or What's App exchanges between colleagues, especially those that take place between a group of colleagues. Please do not identify children in these messages, or staff without their permission
- The school should not be named as your place of work, and no reference to your day at work can be made.
- Staff should not share anything which could personally identify children, bearing in mind the duty of confidentiality contained in their employment contract and that this could result in the school being in breach of the Data Protection Act.
- It is not appropriate to publish other people's photos or tag them on the internet without their permission.
- Staff have a duty to be aware of the severity of the impact on an individual of sending or uploading unkind or inappropriate content, particularly when a wider audience views the content.
- Staff should not have past or current parents/carers as Facebook or WhatsApp friends. If staff have contact details of parents/carers because they work with their child, the headteacher must be notified, and any such contact must remain professional. This is similar if parents/carers are working in school, staff contact can be friendly and informal but it must remain professional.
- Staff should understand the need to use strictest privacy settings on social networking sites to prevent access by parents or carers, both past and present, and to understand the pitfalls of your site being linked to from their friends' sites. Training in privacy settings will be offered to those needing it.

Staff – Email

- All staff will be using **e-mail for school** purposes and will be set up with an e-mail address like this – john.smith@oakleigh.barnet.sch.uk. You need to check your emails regularly.
- Personal business should be conducted on personal emails, not the school one. This may not include personal or sensitive data relating to the school or to any of its pupils.
- Emails should use the same professional language as in a letter on school headed paper.
- Be careful when using 'reply all' as all the recipients will be able to read the whole exchange. NB

Delete conversation trail if it contains confidential items and to avoid sharing school business with outside professionals.

- Staff are **responsible for all e-mails** sent and for any contacts that result in e-mails being received.
- Any unpleasant material or messages received by anyone should be **reported** to the Headteacher, or member of the Senior Leadership Team.
- **Pupil surnames should not be used in emails**. Only first names in the body of the email, and just initials in the Subject box.

Staff - Data Protection

- **STAFF WILL NOT under any circumstances put photographs of children in e-mail exchanges or post photographs on the website, unless permission has been given** by the parents/carers & recorded in writing. If photos are needed surrounding a special event, the Headteacher and Governors in consultation with the parents will decide in relation to this. Check individual **publicity permissions, stored in General information on server.**
- Staff must **log in and out** every time they use a networked PC or laptop. Individual passwords must **not** be given to any other person, apart from ICT support. Class or staff logins are for staff only. Students or volunteers should be **supervised** when accessing class PCs. Staff may not allow **unauthorised** individuals to access email, internet, or network (shared area) or other school systems.
- The **Freedom of Information** Act makes provision for anyone to have access to information held on them. This includes information held in e-mail folders, or communicated on social networking sites, such as Face book etc.
- Do not share your **personal phone numbers**, addresses or any other sensitive information with pupils or parents/carers, unless in situation covered above.
- Make sure your **passwords are strong**, and do not share them with anyone – depending on the information the passwords protect, change them regularly.
- Make sure any removable media containing personal or sensitive information are **encrypted** with passwords. If using external media such as encrypted memory sticks or hard drives on home computers, these must have up-to-date virus protection. Remote access to the server is preferable as it is more secure.
- Laptops need to be brought in regularly to receive Windows Updates.

Staff - Mobiles

- **Mobile phones** should be kept in locker/cupboard, & **switched off** when in class, not on you in person. In staffroom, it is ok to text or to make appropriate use of internet, **no phone calls** to be answered in staffroom/corridors. Calls to be taken outside front entrance only. In exceptional circumstances staff can request to keep their phone on silent with them. This is agreed by the Headteacher or in her absence a member of the SLT.
- Staff will not take **pictures of pupils** using their phones. Any pictures of staff should only be taken with that member of staff's explicit permission, outside of work hours. Photos/video of pupils for work purposes are taken using school devices such as iPads, then transferred to the secure server. NHS professionals/Family support workers can use encrypted work mobiles to take photos/video where necessary.
- Staff must not use mobile devices to send **inappropriate messages, images** or recordings.
- Personal and school-owned mobile devices should not contain any **inappropriate or illegal content**.
- Staff should **not use mobile devices to communicate with parents**. Any contact with parents will be done through authorised school contact channels, such as school telephone or email. In the rare cases when it is necessary to use a personal mobile, use 141 in front of the number you

are dialling so that your number cannot be seen. Staff who work with families outside of school sign the declaration form and alert the Headteacher if they feel the content of any messages are inappropriate or go against the school's Use of Social Media Policy

- On educational visits, where possible staff should **communicate via walkie talkies**. The teacher will have their own mobile.
- If the teacher deems it necessary for other staff to have mobile devices, as a backup means of communication, this will be decided on a case by case basis, and staff members taking mobiles will be listed on the risk assessment, which should be given to the Risk Assessment co-ordinator in advance of the visit. However, **camera phones should not be taken into toileting areas**, unless in emergencies or if the walkie talkie does not work, and then only with two staff present.
- If using personal mobiles on home visits, they cannot be used for taking photos of children or family members. A school camera is preferable for all photos. However, the Family Support team can use Barnet encrypted phones when offsite to take photos for the families they support.

Staff – Reporting Misuse & Adherence to Guidelines

- Staff will report any accidental misuse or incident in relation to use of social media or devices immediately to the Headteacher or member of the SLT

Visitors

Visitors are expected to follow school policy. When signing in, visitors are asked not to use mobile phones on site. In practice, visiting professionals and parents/carers may use their mobiles in office spaces or at entrance. If visitors start to use their phones in classes, staff will ask them to use an appropriate designated space. Visitors including parents/carers cannot take photos of children other than their own.

7. 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.

Parents will be encouraged to monitor their child when using devices as due to their complex needs they may not be able to disclose if something comes up on their screen that is inappropriate or they do not like.

8. Internet access

All members of the school community will be encouraged to use the school's internet network, instead of 3G, 4G and 5G networks, as the network has appropriate filtering and monitoring to ensure individuals are using the internet appropriately.

9. Filtering and monitoring online activity

The governing body 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 body will ensure 'over blocking' does not lead to unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

Reviewed by Emily Wharton January 2026/Approved by FGB 2.2.26
To be reviewed January 2027

The DSL will ensure that specific roles and responsibilities are identified and assigned to manage filtering and monitoring systems and to ensure they meet the school's safeguarding needs.

The Headteacher and ICT technicians will ensure providers e.g. LGFL meet DFE recommended requirements to determine what filtering and monitoring systems are required. 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.

Requests regarding making changes to the filtering system will be directed to the Headteacher. Any changes made to the system will be recorded by LGFL. Reports of inappropriate websites or materials will be made to an ICT technician immediately, who will investigate the matter and makes any necessary changes and report to ISP when appropriate.

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.

9. 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.

Staff 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. 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.

Users will inform ICT technicians if they forget their login details, who will arrange for the user to have a reset password. 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 Headteacher 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.

Full details of the school's network security measures can be found in the Cyber-security Policy.

10. Emails

Access to and the use of emails will be managed in line with the Data Protection Policy,

Staff 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. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

Staff members will be required to block spam and junk mail, and report the matter to ICT technicians. Chain letters, spam and all other emails from unknown sources will be deleted without being opened. ICT technicians will organise training for staff where they explain what a phishing email and other malicious emails might look like – this training will include information on the following:

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

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

11. Social networking

The use of social media by staff and parents will be managed in line with the school's Use of Social Media Policy.

12. The school website

The Headteacher 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.

13. Monitoring and review

The school recognises that the online world is constantly changing; therefore, the DSL, ICT technicians and the Headteacher conduct **half-termly** light-touch reviews of this policy to evaluate its effectiveness.

The governing board, Headteacher and DSL will review this policy in full on an **annual** basis and following any online safety incidents.

The next scheduled review date for this policy is **January 2027**

All changes made to policy are communicated to all members of the school community

Reviewed by Emily Wharton January 2026/Approved by FGB 2.2.26
To be reviewed January 2027

Online harms and risks – curriculum coverage

Subject area	Description and teaching content	Curriculum area the harm or risk is covered in
How to navigate the internet and manage information		
Age restrictions	Some online activities have age restrictions because they include content which is not appropriate for children under a specific age. Teaching will include 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 will be covered in the following curriculum areas: • Health education • Computing
How content can be used and shared	Knowing what happens to information, comments or images that are put online. Teaching will include 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 will be covered in the following curriculum areas: • Relationships education
Disinformation, misinformation and hoaxes	Some information shared online is accidentally or intentionally wrong, misleading or exaggerated. Teaching will include the following: • Disinformation and why individuals or groups choose to share false information in order to deliberately deceive • Misinformation and being aware that false and misleading information can be shared inadvertently • Misinformation and understanding that some genuine information can be published with the	This risk or harm will be covered in the following curriculum areas: • Relationships and health education • **[KS2 and above]** Computing •

	deliberate intent to harm, e.g. releasing private information or photographs • 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	
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 will include 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, or groomed as a result of interacting with a fake website or scam email • Who pupils should go to for support • The risk of 'too good to be true' online offers, advertising and fake product sales designed to persuade people to part with money for products and services that do not exist	This risk or harm will be covered in the following curriculum areas: • Relationships education
Online fraud	Fraud can take place online and can have serious consequences for individuals and organisations. Teaching will include the following: • What identity fraud, scams and phishing are • That online fraud can be highly sophisticated and that anyone can be a victim • How to protect yourself and others against different types of online fraud • How to identify 'money mule' schemes and recruiters • The risk of online social engineering to facilitate authorised push payment fraud, where a victim is tricked into sending a payment to the criminal • The risk of sharing personal information that could be used by fraudsters • That children are sometimes targeted to access adults' data	This risk or harm will be covered in the following curriculum areas: • Relationships education

	• What 'good' companies will and will not do when it comes to personal details • How to report fraud, phishing attempts, suspicious websites and adverts	
Password phishing	Password phishing is the process by which people try to find out individuals' passwords so they can access protected content. Teaching will include the following: • 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	This risk or harm will be covered in the following curriculum areas: • Relationships education •
Personal data	Online platforms and search engines gather personal data – this is often referred to as 'harvesting' or 'farming'. Teaching will include 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 will be covered in the following curriculum areas: • Relationships education
Persuasive design	Many devices, apps and games are designed to keep users online for longer than they might have planned or desired. Teaching will include the following: • That the majority of games and platforms are designed to make money, and that their primary driver is to encourage people to stay online for as long as possible to encourage them to spend money or generate advertising revenue • How notifications are used to pull users back online	This risk or harm will be covered in the following curriculum areas: • Health education • Computing
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 will include the following: • How to find information about privacy settings on various sites, apps, devices and platforms	This risk or harm will be covered in the following curriculum areas: • Relationships education

	• That privacy settings have limitations	
Targeting of online content	Much of the information seen online is a result of some form of targeting. Teaching will include 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 will be covered in the following curriculum areas: • Relationships education
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 will include 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 will be covered in the following curriculum areas: • Relationships education
Radicalisation	Pupils are at risk of accessing inappropriate and harmful extremist content online, including terrorist material. Extremist and terrorist groups use social media to identify and target vulnerable individuals. Teaching will include the following: • How to recognise extremist behaviour and content online • Which actions could be identified as criminal activity • Techniques used for persuasion • How to access support from trusted individuals and organisations	All areas of the curriculum
Challenges	Online challenges acquire mass followings and encourage others to take part in what they suggest. Teaching will include the following:	This risk or harm will be covered in the following curriculum areas:

	• 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 • How and where to go for help • The importance of telling an adult about challenges which include threats or secrecy, such as 'chain letter' style challenges	• Relationships education
Content which incites violence	Knowing that violence can be incited online and escalate very quickly into offline violence. Teaching will include 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 will be covered in the following curriculum areas: • Relationships education
Fake profiles	Not everyone online is who they say they are. Teaching will include 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 will be covered in the following curriculum areas: • Relationships education
Grooming	Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation, gangs and financial exploitation. Teaching will include 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	This risk or harm will be covered in the following curriculum areas: • Relationships education

	being clear it is never the fault of the child who is abused and why victim blaming is always wrong.	
Livestreaming	Livestreaming (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 will include the following: • What the risks of carrying out livestreaming are, e.g. the potential for people to record livestreams and share the content • 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 • 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 will be covered in the following curriculum areas: • Relationships education (as appropriate to level of understanding)
Unsafe communication	Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching will include the following: • That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with • How to identify indicators of risk and unsafe communications • The risks associated with giving out addresses, phone numbers or email addresses to people pupils do not know, or arranging to meet someone they have not met before • What online consent is and how to develop strategies to confidently say no to both friends and strangers online	This risk or harm will be covered in the following curriculum areas: • Relationships education
Wellbeing		
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 will include the following: • How to evaluate critically what pupils are doing online, why they are doing it and for how long (screen time)	This risk or harm will be covered in the following curriculum areas: • Health education

	• 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 due to 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	
Online vs. offline behaviours	People can often behave differently online to how they would act face to face. Teaching will include the following: • How and why people can often portray an exaggerated picture of their lives (especially online) and how that can lead to pressure 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 will be covered in the following curriculum areas: • Relationships education