Newman School

Online Safety Policy

Date policy last reviewed: 06.11.2023

Signed by:

Michaela Glarvey

Headteacher Date:

Roz Danks

Chair of governors Date:

Last updated: 06.11.23

Contents:

Statement of intent

1. Legal framework
2. Roles and responsibilities
3. Managing online safety
4. Cyberbullying
5. Peer-on-peer 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. **[New]** Use of smart technology
14. Educating parents
15. Internet access
16. Filtering and monitoring online activity
17. Network security
18. Emails
19. Social networking
20. The school website
21. Use of devices
22. Remote learning
23. Monitoring and review

Appendices

A. Online harms and risks – curriculum coverage

Statement of intent

Newman 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 (2021) 'Harmful online challenges and online hoaxes'
- DfE (2023) 'Keeping children safe in education 2023'
- Department for Digital, Culture, Media and Sport and UK Council for Internet Safety (2020) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- DfE (2019) 'Teaching online safety in school'
- DfE (2022) 'Searching, screening and confiscation'
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'
- UK Council for Child Internet Safety (2018) 'Using External Visitors to Support Online Safety Education`
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'

This policy operates in conjunction with the following school policies:

- Social Media Policy
- It & Communication Policy
- Allegations of Abuse Against Staff Policy
- Acceptable Use Policy
- Data Breach incident Reporting Policy
- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- PSHE / SRE Policy
- Staff Code of Conduct
- Parent, Carer, Visitor and Governor's Code of Conduct
- Behaviour & Relationships Policy
- Grievance Procedures Policy
- Data Protection Policy
- Confidentiality & Information Sharing Policy
- Device User Agreement
- Remote Learning Policy
- Technology Acceptable Use Agreement for Pupils
- Technology Acceptable Use Agreement for Pupils (Widgit Version)
- Technology Acceptable Use Agreement for Staff & Governors
- Technology Acceptable Use Agreement for Visitors
- Communication Guidance

2. Roles and responsibilities

The Governing Board are responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an **annual** basis.
- Ensuring their own knowledge of online safety issues is up to date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

The Headteacher / DSL is responsible for:

- Ensuring that online safety is a running and interrelated theme throughout the school's policies and procedures, including in those related to the curriculum, teacher training and safeguarding.
- Supporting the DSL and the deputy DSL by ensuring they have enough time and resources to carry out their responsibilities in relation to online safety.
- Ensuring staff receive regular, up-to-date, and appropriate online safety training and information as part of their induction and safeguarding training.
- Ensuring online safety practices are audited and evaluated.
- Supporting staff to ensure that online safety is embedded throughout the curriculum so that all pupils can develop an appropriate understanding of online safety.
- Organising engagement with parents to keep them up to date with current online safety issues and how the school is keeping pupils safe.
- Working with the Deputy DSL's and SIRO Committee 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 Deputy DSL's and SIRO Committee are responsible for:

- Taking the lead responsibility for online safety in the school.
- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Ensuring appropriate referrals are made to external agencies, as required.
- Keeping up to date with current research, legislation, and online trends.
- Coordinating the school's participation in local and national online safety events, e.g. Safer Internet Day.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff.

- Ensuring all members of the school community understand the reporting procedure.
- Maintaining records of reported online safety concerns as well as the actions taken in response to concerns.
- Monitoring online safety incidents to identify trends and any gaps in the school's provision and using this data to update the school's procedures.
- Reporting to the governing board about online safety on a **termly** basis.
- Working with the headteacher and SIRO to conduct **half-termly** light-touch reviews of this policy.
- Working with the headteacher and governing board to update this policy on an **annual** basis.
- Implementing appropriate security measures as directed by the headteacher.
- Working with the DSL and headteacher to conduct half-termly light-touch reviews of this policy.

Bluebox IT is responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.

All staff members are responsible for:

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

Pupils are responsible for:

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

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

- Staff 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
- Educational Drama Productions are conducted on the topic of remaining safe online, as appropriate to the cohort.

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 and recorded on CPOMS.

Concerns regarding a staff member's online behaviour are reported to the headteacher, who decides on the best course of action in line with the relevant policies, e.g. the Staff Code of Conduct, Allegations of Abuse Against Staff Policy, and Disciplinary Policy and Procedures. If the concern is about the headteacher, it is reported to the chair of governors.

Concerns regarding a pupil's online behaviour are reported to the Deputy DSL, who investigates concerns with relevant staff members, e.g. the headteacher and SIRO Committee, and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behavioural & Relationship Policy, Parent, Carer and Visitors Code of Conduct and Safeguarding Policy.

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

The school avoids unnecessarily criminalising pupils, e.g. calling the police, where criminal behaviour is thought to be inadvertent and because 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 and DDSLs.

4. Cyberbullying

Cyberbullying can include the following:

- Threatening, intimidating, or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible

- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Menacing or upsetting responses to someone in a chatroom
- Unpleasant messages sent via instant messaging
- Unpleasant or defamatory information posted to blogs, personal websites, and social networking sites, e.g. Facebook

Cyberbullying against pupils or staff is not tolerated under any circumstances. Incidents of cyberbullying are dealt with quickly and effectively wherever they occur in line with the 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 and off and online and will remain aware that pupils are less likely to report concerning online sexual behaviours, particularly if they are using websites that they know adults will consider to be inappropriate for their age.

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

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

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

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

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, including the following:

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

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

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

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

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

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

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

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 Safeguarding 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 / DDSL without delay, who will handle the situation in line with the Safeguarding Policy

7. Mental health

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

Staff will be aware that online activity both in and outside of school can have a substantial impact on a pupil's mental state, both positively and negatively. 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.

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 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 / SIRO Committee member immediately.

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

The DSL / SIRO Committee 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 regarding 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 DDSLs and curriculum team will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully, and will ensure that pupils cannot access sites or areas of the internet that may encourage them to stray from lawful use of

technology, e.g. the 'dark web', on school-owned devices or on school networks through the use of appropriate firewalls.

10. Online safety training for staff

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

Information about the school's full responses to online safeguarding incidents can be found in the Anti-bullying Policy and Safeguarding Policy (which includes child on child abuse and child protection).

11. Online safety and the curriculum

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

[List the subjects in which your school specifically covers online safety – examples have been provided for you.]

- RSE
- Health education
- PSHE
- Citizenship
- Computing / 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
- What healthy and respectful relationships, including friendships, look like
- Body confidence and self-esteem
- Consent, e.g. with relation to the sharing of indecent imagery or online coercion to perform sexual acts
- Acceptable and unacceptable online behaviour
- How to identify online risks
- How and when to seek support
- How to identify when something is deliberately deceitful or harmful
- How to recognise when something they are being asked to do puts them at risk or is age-inappropriate

The 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 is 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.

The school recognises that, while any pupil can be vulnerable online, there are some pupils who may be more susceptible to online harm or have less support from family and friends in staying safe online, e.g. pupils with SEND and LAC. Relevant members of staff, e.g. the form teacher and designated teacher for LAC, work together to ensure the curriculum is tailored so these pupils receive the information and support they need.

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

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

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

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.

Before conducting a lesson or activity on online safety, the class teacher considers 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. Lessons and activities are 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 ensures 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 is used during lessons, including the following:

[List the technology used in lessons – this list does not need to be exhaustive. An example has been provided for you.]

- Computers
- Laptops
- Ipads / Tablets
- Intranet
- Email
- Cameras

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

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

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.

Staff will use all smart technology and personal technology in line with the school's Staff Acceptable Use Policy.

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 the pupil AUP, therefore pupils will not be permitted to use smart devices or any other personal technology in school.

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.

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 and Physical Interventions Policy and a referral out to the Targeted Action Group for further interventions.

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.

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 4C's (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

Newman school works in partnership with parents to ensure pupils stay safe online at school and at home. Parents are provided with information about the school's approach to online safety and their role in protecting their children. Parents are 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 many 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 is raised in the following ways:

- Parents' evenings
- Newsletters
- Online resources
- EHCP Annual Reviews

15. Internet access

Pupils, staff, and other members of the school community are only granted access to the school's internet network once they have read and signed the Acceptable Use Agreement. A record is kept of users who have been granted internet access in the school office. Only devices approved by the Headteacher should be permitted to be connected to the network, either through wired or wireless connectivity. Where devices are connected to the network using wireless, the wireless network should be secure; as a minimum this should be done using WPA. Open Access Wireless Access Points must not be connected to the school's network. Encryption is applied to wireless networks; encryption keys should be kept secure and changed at least termly. Mobile devices may with permission connect to the network but in full compliance with the ICT policies and this permission may be withdrawn at any time.

16. Filtering and monitoring online activity

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

The Headteacher and SIRO Committee undertake a risk assessment to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements are appropriate to pupils' ages and SEND needs, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks. ICT technicians undertake **monthly** checks on the filtering and monitoring systems to ensure they are effective and appropriate. Updates will be applied to the Smoothwall Monitoring system as and when released by the vendor. Policy changes, or changes to Allow and Block lists will be completed by the technician when authorised by the appropriate school authority. This process requires review and clarification by the SIRO committee.

Requests regarding making changes to the filtering system are directed to the SIRO Committee. Prior to making any changes to the filtering system, SIRO and the DSL conduct a risk assessment. Reports of inappropriate websites or materials are made via CPOMs to the SIRO Committee / site leads immediately, who investigate the matter and makes any necessary follow up actions.

Deliberate breaches of the filtering system are reported to the SIRO Committee / site leads, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behavioural Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Staff Code of Conduct Policy.

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), Child Exploitation and Online Protection (CEOP) and/or the police.

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

17. Network security

Technical security features, such as anti-virus software, are kept up-to-date and managed by ICT technicians. Firewalls are always switched on. ICT technicians review the firewalls on a weekly basis to ensure they are running correctly, and to carry out any required updates. Sophos AV software is managed by technicians through the schools Sophos portal. Virus definitions are automatically updated through this portal and applied to agents and installed on school devices.

Firewalls are always on, and firmware will update as and when required. Technicians will review functionality on a regular basis to ensure continued availability.

Staff and pupils are advised not to download unapproved software or open unfamiliar email attachments and are expected to report all malware and virus attacks to the SIRO Committee.

All members of staff have their own unique usernames and private passwords to access the school's systems. Pupils across the school are provided with their own unique username and private passwords, where appropriate. Staff members and pupils are responsible for keeping their passwords private. Passwords have a minimum and maximum length and require a mixture of letters, numbers, and symbols to ensure they are as secure as possible. Users are required to change their password termly. Passwords should be memorised and if written down MUST not be kept with the device in any form.

Users inform relevant staff if they forget their login details, who will arrange for the user to access the systems under different login details. Users are not permitted to share their login details with others and are not 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 is informed and decides the necessary action to take.

Users are 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 Data Breach policy.

18. Emails

Access to and the use of emails is managed in line with the Data Protection Policy and the Pupil, Staff and Visitor Acceptable Use Policies.

Staff and pupils are given approved school email accounts and are only able to use these accounts at school and when doing school-related work outside of school hours. Prior to being authorised to use the email system, staff and pupils must agree to and sign the Acceptable Use Agreement. Personal email accounts are not permitted to be used on the school site. Any email that contains sensitive or personal information is only sent using secure and encrypted email. Emails created or received as part of the school business will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000.

Staff members and pupils are required to block spam and junk mail and report the matter to the SIRO Committee. The school's monitoring system can detect inappropriate links, malware, and profanity within emails – staff and pupils are made aware of this. Chain letters, spam and all other emails from unknown sources are deleted without being opened. Microsoft 365 has an ongoing policy to review incoming emails to school which provides a dynamic search and deletion of any message containing potentially offensive words and profanities. The school's Impero solution will alert nominated staff to the presence of similar content in emails being sent from the school email system.

Any cyber-attacks initiated through emails are managed in line with the Emergency Plan.

19. Social networking

Personal use

Access to social networking sites is filtered as appropriate. Staff and pupils are not permitted to use social media for personal use during lesson time. Staff members are advised that their

conduct on social media can have an impact on their role and reputation within the school. The Staff Code of Conduct contains information on the acceptable use of social media – staff members are required to always follow these expectations.

Staff receive **annual** training on how to use social media safely and responsibly. Staff are not permitted to communicate with pupils or parents over social networking sites and are reminded to alter their privacy settings to ensure pupils and parents are not able to contact them on social media. Where staff have an existing personal relationship with a parent or pupil, and thus are connected with them on social media, e.g. they are friends with a parent at the school, they will disclose this to the DSL and headteacher and will ensure that their social media conduct relating to that parent is appropriate for their position in the school.

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

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

Use on behalf of the school

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

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

20. The school website

The 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.

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

21. Use of devices

School-owned devices

Staff members may be issued with the following devices to assist with their work:

- Laptop
- Tablet
- Mobile Phone

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

School-owned devices are used in accordance with the Acceptable User Agreement. All school-owned devices are password protected. All school-owned devices are fitted with software to ensure they can be remotely accessed in case data on the device needs to be protected, retrieved, or erased.

ICT technicians review all school-owned devices to carry out software updates and ensure there is no inappropriate material or malware on the devices. School owned Windows devices are patched in line with regular security updates as and when released. Staff should not have access to local admin rights on school devices so that all software installation is controlled through the local technician or Bluebox IT support desk.

Cases of staff members or pupils found to be misusing school-owned devices will be managed in line with the Staff Code of Conduct Policy and Behaviour and Relationships Policy, respectively.

Personal devices

Personal devices are used in accordance with the following guidelines.

Newman School allows staff, including temporary and peripatetic staff, and visitors to use personal mobile phones and devices only in designated areas and never in the presence of students. Under no circumstance does the school/college allow a member of staff to contact a student or parent/carer using their personal device.

Parents/carers may only use personal mobile phones and devices in designated areas unless otherwise informed, e.g. for specific events and activities such as Grandparents are invited to the school nativity play and wish to video it. These images are for personal use and the Data Protection Act does not apply. Under no circumstance should images be taken at any time on school/ college premises or on off-site school/ college events and activities of anyone other than their own child unless there is a pre-specified permission from the Headteacher. When a parent/carer is on school/college premises but not in a designated area, their phone/s must be kept out of sight and on silent mode.

Students are allowed to bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. In lesson times all such devices must be switched off and handed in at reception. Under no circumstance should students use their personal mobile devices/phones to take images of

- any other student unless they and their parents have given agreement in advance
- any member of staff

The school/college is not responsible for the loss, damage, or theft on school premises of any personal mobile device.

Users bringing personal devices into school/ college must ensure there is no inappropriate or illegal content on the device.

There are four main systems Newman School permits to be used on personal devices as they are of major benefit to the running of the school/ college and safeguarding of the students. There systems are stated below along with the main rules that accompany personal device usage in order to protect users and the personal data of everyone involved:

- CPOMS Safeguarding System
- Outlook
- 3CX
- Evidence Me

Guidelines applicable to all systems:

If you have been issued with a business device this must always take priority for remote working use.

If your personal device is lost or stolen, you must immediately alert school so appropriate security procedures can be initiated.

There is an expectation that due to the installation of these school/ college applications that you will have a secure PIN on your personal device. Finally, please be mindful of personal data held within these applications and the risk associated such as unauthorised access if your personal device is shared with individuals such as family members.

Guidelines that are application specific:

<u>3CX:</u>

When on school/ college business contact must always be made via the 3CX solution and not through personal devices.

Ensure you never store parent/ carer/ student phone numbers in your personal devices contact list

<u>Outlook:</u>

We will only accept use of work emails via downloading the official Microsoft Outlook application from Microsoft Corporation.

<u>Evidence Me:</u>

At no point should photographs be stored on personal devices to upload to the app at a later date, if you accidentally take the photo on your personal device first and then upload to the app you must ensure immediate deletion.

CPOMS:

Ensure you click ‘log out’ after each session you use the application on your personal device.

Staff members report concerns about their colleagues’ use of personal devices on the school premises in line with the Allegations of Abuse Against Staff Policy. If a member of staff is thought to have illegal content saved or stored on a personal device, or to have committed an offence using a personal device, the headteacher will inform the police and action will be taken in line with the Allegations of Abuse Against Staff Policy.

If a pupil needs to contact their parents during the school day, they are allowed to use the phone in the school office. The Headteacher may authorise the use of mobile devices by a pupil for safety or precautionary use.

Pupils’ devices can be searched, screened, and confiscated in accordance with the Behaviour and Interventions Policy. If a staff member reasonably believes a pupil’s personal device has been used to commit an offence or may provide evidence relating to an offence, the device will be handed to the police.

Visitors to the school are given an AUP to inform them of the expected use of personal devices. Any concerns about visitors’ use of personal devices on the school premises are reported to the DSL.

22. Remote learning

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

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

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

Remote, offsite backup is not aligned to all devices/data currently, however, the Redstor RBBUS solution only backs up 'Critical' data (as defined by the school). An onsite backup is used to backup all school server data. Individual remote devices will not be backed up and any data created on these devices locally will not be able to be recovered if deleted, unless saved on the server (via a VPN connection) or to Microsoft 365 - in the cloud.

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

- Reinforce the importance of children staying safe online.
- Ensure parents are aware of what their children are being asked to do, e.g. sites they have been asked to use and staff they will interact with.

- Encourage them to set age-appropriate parental controls on devices and internet filters to block malicious websites.
- Direct parents to useful resources to help them keep their children safe online.

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

23. Monitoring and review

The school recognises that the online world is constantly changing; therefore, the SIRO Committee, site leads and the Headteacher conduct half-termly light-touch reviews of this policy to evaluate its effectiveness.

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

The next scheduled review date for this policy is October 2024.

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

NEWMAN SCHOOL
KS3-5
PSHE CURRICULUM COMPLIANCE WITH DfE ONLINE SAFETY IN SCHOOLS

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	SELF CARE SUPPORT AND SAFETY - SS4 KEEPING SAFE ONLINE (pg 127) **"**Describe what keeping safe online"
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)	SELF CARE SUPPORT AND SAFETY - SS4 KEEPING SAFE ONLINE (pg 127) "Identify what we should do before we 'like', 'forward' or 'share' on social media and how this helps to keep us safe online." "Explain rules for keeping safe when using different social media platforms." SELF CARE SUPPORT AND SAFETY - SA4 – MANAGING PRESSURE (PG 124) "Identify some of the ways in which pressure might be put on us by other people, including online." "Describe strategies that can be used if someone is using pressure to persuade

		us to do something, including online." SELF CARE SUPPORT AND SAFETY - SS6 PUBLIC AND PRIVATE (PG 128) "Identify what is appropriate and inappropriate to share online." "Identify trusted adults who can help us if someone tries to pressurise us online." "Explain how to manage requests to share a photo, or information about ourselves or others online, including how to report." "Describe specific ways of keeping ourselves safe online (e.g. secure passwords, never giving out personal details or passwords, not lending our mobile phone, covering our computer's camera when not in use)." "Recognise that sharing and/or viewing sexual images of anyone under 18 (including those created by anyone under 18) is against the law." "Explain what could happen next (e.g. police involvement, parent/carer involvement, prosecution)

		and the impact on self and others."
Disinformation, misinformation and hoaxes	Some information shared online is accidentally or intentionally wrong, misleading or exaggerated. Teaching includes the following: • Disinformation and why individuals or groups choose to share false information in order to deliberately deceive • Misinformation and being aware that false and misleading information can be shared inadvertently • Online hoaxes, which can be deliberately and inadvertently spread for a variety of reasons • 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	SELF CARE SUPPORT AND SAFETY - SS4 KEEPING SAFE ONLINE (pg 127) "Recognise that not all information seen online is true." "Identify some ways in which we can recognise when we are being manipulated by online content or contact, and ways to respond." "Explain how other people's identity online can be different from what it actually is in real life." THE WORLD I LIVE IN WILI2 – MANAGING ONLINE INFORMATION (PG 139) "Recognise that not everything we see online is 'real' or 'true'." "Recognise that not everything we see or read online is trustworthy;that some things that are written about are not real and are 'fake'." "Explain the influence that fake news can have on people's opinions, attitudes to others and understanding of the world."
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	SELF CARE SUPPORT AND SAFETY -

	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, or groomed as a result of interacting with a fake website or scam email • Who pupils should go to for support	SS4 KEEPING SAFE ONLINE (pg 127) "Recognise that data about us can be collected online, and used, for example, to determine what information and advertising we are shown" "Identify some ways in which we can recognise when we are being manipulated by online content or contact, and ways to respond." "Identify some ways in which we can recognise when we are being manipulated by online content or contact, and ways to respond." "Describe or demonstrate help-seeking strategies to support online safety (e.g. knowing how to block people on social media, using the CEOP report button)." SA4 – MANAGING PRESSURE (PG 124) "Identify some of the ways in which pressure might be put on us by other people, including online." "Describe strategies that can be used if someone is using pressure to persuade us to do something, including online." SELF CARE SUPPORT AND SAFETY -

		SS6 PUBLIC AND PRIVATE (PG 128) "Explain that there are online 'scams' (ways that people may try to trick us online); identify what some of these ways of deceiving people might be (e.g. phishing, fake email addresses)." THE WORLD I LIVE IN WILI2 – MANAGING ONLINE INFORMATION (PG 139) "Describe simple steps to take to check if something we see online is trustworthy." "Identify organisations/ websites that can help us or other people with concerns about something seen or experienced online." "Explain that information from our internet use is gathered, stored and used by external Organisations"
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	SELF CARE SUPPORT AND SAFETY - SS4 KEEPING SAFE ONLINE (pg 127) "Recognise that data about us can be collected online, and used, for example, to determine what information and

		advertising we are shown" "Identify some ways in which we can recognise when we are being manipulated by online content or contact, and ways to respond." THE WORLD I LIVE IN WILI2 – MANAGING ONLINE INFORMATION (PG 139) "Describe simple steps to take to check if something we see online is trustworthy." "Identify organisations/ websites that can help us or other people with concerns about something seen or experienced online." "Explain that information from our internet use is gathered, stored and used by external organisations."
Password phishing	Password phishing is the process by which people try to find out individuals' passwords so they can access protected content. Teaching includes the following: • Why passwords are important, how to keep them safe and that others might try to get people to reveal them • 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	SELF CARE SUPPORT AND SAFETY - SS4 KEEPING SAFE ONLINE (pg 127) "Recognise that data about us can be collected online, and used, for example, to determine what information and advertising we are shown" "Explain rules for keeping

		safe when using different social media platforms." "Describe or demonstrate help-seeking strategies to support online safety (e.g. knowing how to block people on social media, using the CEOP report button)." SELF CARE SUPPORT AND SAFETY - SS6 PUBLIC AND PRIVATE (PG 128) "Explain that there are online 'scams' (ways that people may try to trick us online); identify what some of these ways of deceiving people might be (e.g. phishing, fake email addresses)."
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	SELF CARE SUPPORT AND SAFETY - SS4 KEEPING SAFE ONLINE (pg 127) "Recognise that data about us can be collected online, and used, for example, to determine what information and advertising we are shown" "Explain rules for keeping safe when using different social media platforms." "Describe or demonstrate help-seeking strategies to support online safety

		(e.g. knowing how to block people on social media, using the CEOP report button)." THE WORLD I LIVE IN WILI2 – MANAGING ONLINE INFORMATION (PG 139) "Explain that information from our internet use is gathered, stored and used by external organisations."
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, and that their primary driver is to encourage people to stay online for as long as possible • How notifications are used to pull users back online	SELF CARE SUPPORT AND SAFETY - SS4 KEEPING SAFE ONLINE (pg 127) "Explain some steps we can take to take care of our own and other people's safety and wellbeing when using social media." THE WORLD I LIVE IN WILI2 – MANAGING ONLINE INFORMATION (PG 139) "Recognise that advertising online is targeted at individuals."
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	SELF CARE SUPPORT AND SAFETY - SS4 KEEPING SAFE ONLINE (pg 127) "Recognise that data about us can be collected

		online, and used, for example, to determine what information and advertising we are shown"
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	SELF CARE SUPPORT AND SAFETY - SS4 KEEPING SAFE ONLINE (pg 127) "Recognise that data about us can be collected online, and used, for example, to determine what information and advertising we are shown" THE WORLD I LIVE IN WILI2 – MANAGING ONLINE INFORMATION (PG 139) "Recognise that advertising online is targeted at individuals." "Identify some of the techniques that advertisers might use to get our attention or persuade us to believe something is true, and what their motives might be." "Explain that information from our internet use is gathered, stored and used by external organisations."
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	SELF CARE SUPPORT AND SAFETY - SS4 KEEPING SAFE ONLINE (pg 127) "Identify some possible risks of using social media." "Describe how we can respond, including getting help, if we see or are sent upsetting or inappropriate online content." "Explain some steps we can take to take care of our own and other people's safety and wellbeing when using social media." "Identify some ways in which we can recognise when we are being manipulated by online content or contact, and ways to respond." "Describe or demonstrate help-seeking strategies to support online safety (e.g. knowing how to block people on social media, using the CEOP report button)." SELF AWARENESS - SA4 – MANAGING PRESSURE (PG 124) "Identify some of the ways in which pressure might be put on us by other people, including online." "Describe strategies that can be used if someone is using pressure to persuade

		us to do something, including online."
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 • 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	SELF CARE SUPPORT AND SAFETY - SS4 KEEPING SAFE ONLINE (pg 127) "Identify some ways in which we can recognise when we are being manipulated by online content or contact, and ways to respond." "Describe how we can respond, including getting help, if we see or are sent upsetting or inappropriate online content." "Explain some steps we can take to take care of our own and other people's safety and wellbeing when using social media." "Describe some ways in which social media can be used in a safe and positive way." "Identify what we should do before we 'like', 'forward' or 'share' on social media and how this helps to keep us safe online." "Identify some possible risks of using social media." SELF AWARENESS – SA4 – MANAGING PRESSURE (PG 124) "Identify some of the ways

		in which pressure might be put on us by other people, including online." "Describe strategies that can be used if someone is using pressure to persuade us to do something, including online."
Content which incites violence	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	SELF CARE SUPPORT AND SAFETY - SS4 KEEPING SAFE ONLINE (pg 127) "Identify some ways in which we can recognise when we are being manipulated by online content or contact, and ways to respond." "Describe or demonstrate help-seeking strategies to support online safety(e.g. knowing how to block people on social media, using the CEOP report button)." "Describe the risks and law relating to carrying a weapon." "Describe how to recognise the difference between friendship groups and gangs; describe some of the risks of becoming part of a gang." SELF AWARENESS - SA4 – MANAGING PRESSURE (PG 124)

		"Identify some of the ways in which pressure might be put on us by other people, including online." "Describe strategies that can be used if someone is using pressure to persuade us to do something, including online." "Identify reasons why we might put ourselves under pressure, and how others may apply pressure or encourage us to join a group or a gang; exit strategies and how to access appropriate support."
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	SELF CARE SUPPORT AND SAFETY - SS4 KEEPING SAFE ONLINE (pg 127) "Recognise that not all information seen online is true." "Explain how other people's identity online can be different from what it actually is in real life."" "Identify some possible risks of using social media." "Identify sources of advice and support, and ways to report online concerns."

		SELF CARE SUPPORT AND SAFETY - SS6 PUBLIC AND PRIVATE (PG 128) "Describe specific ways of keeping ourselves safe online (e.g. secure passwords, never giving out personal details or passwords, not lending our mobile phone, covering our computer's camera when not in use)."
Grooming	Knowing about the different types of grooming and motivations for it, e.g. radicalisation, child sexual abuse and exploitation, and gangs and 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.	SELF CARE SUPPORT AND SAFETY - SS4 KEEPING SAFE ONLINE (pg 127) "Recognise that not all information seen online is true." "Explain how other people's identity online can be different from what it actually is in real life."" "Identify some ways in which we can recognise when we are being manipulated by online content or contact, and ways to respond." "Describe or demonstrate help-seeking strategies to support online safety(e.g. knowing how to block people on social media, using the CEOP report button)." "Explain how other people's identity online

		can be different from what it actually is in real life.”” “Identify some possible risks of using social media.” “Identify sources of advice and support, and ways to report online concerns.” SELF AWARENESS SA4 – MANAGING PRESSURE (PG 124) “Identify some of the ways in which pressure might be put on us by other people, including online.” “Describe strategies that can be used if someone is using pressure to persuade us to do something, including online.” “Identify reasons why we might put ourselves under pressure, and how others may apply pressure or encourage us to join a group or a gang; exit strategies and how to access appropriate support.” SELF CARE SUPPORT AND SAFETY - SS6 PUBLIC AND PRIVATE (PG 128) “Identify what is appropriate and inappropriate to share online.”

		"Identify trusted adults who can help us if someone tries to pressurise us online." "Explain how to manage requests to share a photo, or information about ourselves or others online, including how to report." "Describe specific ways of keeping ourselves safe online (e.g. secure passwords, never giving out personal details or passwords, not lending our mobile phone, covering our computer's camera when not in use)."
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 includes the following: • What the risks of carrying out livestreaming 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	SELF CARE SUPPORT AND SAFETY - SS4 KEEPING SAFE ONLINE (pg 127) "Describe what keeping safe online means." "Explain rules for keeping safe when using different social media platforms." "Identify sources of advice and support, and ways to report online concerns." "Identify some possible risks of using social media." "Describe or demonstrate help-seeking strategies to

		support online safety(e.g. knowing how to block people on social media, using the CEOP report button)." "Explain how other people's identity online can be different from what it actually is in real life."" SELF AWARENESS - SA4 – MANAGING PRESSURE (PG 124) "Identify some of the ways in which pressure might be put on us by other people, including online." "Describe strategies that can be used if someone is using pressure to persuade us to do something, including online." "Identify reasons why we might put ourselves under pressure, and how others may apply pressure or encourage us to join a group or a gang; exit strategies and how to access appropriate support." SELF CARE SUPPORT AND SAFETY - SS6 PUBLIC AND PRIVATE (PG 128) "Identify what is appropriate and inappropriate to share online."

		"Identify trusted adults who can help us if someone tries to pressurise us online." "Explain how to manage requests to share a photo, or information about ourselves or others online, including how to report." "Describe specific ways of keeping ourselves safe online (e.g. secure passwords, never giving out personal details or passwords, not lending our mobile phone, covering our computer's camera when not in use)." "Explain and demonstrate how to ask for help and whom to go to if we have seen something upsetting or done something online that we are now worried about or regret."
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	SELF CARE SUPPORT AND SAFETY - SS6 PUBLIC AND PRIVATE (PG 128) "Recognise that sharing and/or viewing sexual images of anyone under 18 (including those created by anyone under 18) is against the law." CHANGING AND GROWING CG4 – INTIMATE RELATIONSHIPS,

		CONSENT AND CONTRACEPTION (PG 134) "Recognise that the portrayal of sex in the media and social media (including pornography) is an unrealistic representation of sexual behaviour and can affect people's expectations of relationships and sex." "Recognise that viewing pornography can have ongoing harms and where and how to access help if concerned."
Unsafe communication	Knowing different strategies for staying safe when communicating with others, especially people they do not know or have not met. Teaching includes the following: • That communicating safely online and protecting your privacy and data is important, regardless of who you are communicating with • How to identify indicators of risk and unsafe communications • The risks associated with giving out addresses, phone numbers or email addresses to people pupils do not know, or arranging to meet someone they have not met before • What online consent is and how to develop strategies to confidently say no to both friends and strangers online	SELF CARE SUPPORT AND SAFETY - SS4 KEEPING SAFE ONLINE (pg 127) "Describe what keeping safe online means." "Recognise that not all information seen online is true." "Explain how other people's identity online can be different from what it actually is in real life." "Explain rules for keeping safe when using different social media platforms." "Identify sources of advice and support, and ways to report online concerns."

		"Identify how to make safe, reliable choices from search results." "Identify some ways in which we can recognise when we are being manipulated by online content or contact, and ways to respond." "Describe or demonstrate help-seeking strategies to support online safety (e.g. knowing how to block people on social media, using the CEOP report Button)." SELF AWARENESS - SA4 – MANAGING PRESSURE (PG 124) "Identify some of the ways in which pressure might be put on us by other people, including online." "Describe strategies that can be used if someone is using pressure to persuade us to do something, including online." "Identify reasons why we might put ourselves under pressure, and how others may apply pressure or encourage us to join a group or a gang; exit strategies and how to access appropriate support."

		SELF CARE SUPPORT AND SAFETY - SS6 PUBLIC AND PRIVATE (PG 128) "Identify what is appropriate and inappropriate to share online." "Identify trusted adults who can help us if someone tries to pressurise us online." "Describe specific ways of keeping ourselves safe online (e.g. secure passwords, never giving out personal details or passwords, not lending our mobile phone, covering our computer's camera when not in use)."
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	SELF CARE SUPPORT AND SAFETY - SS4 KEEPING SAFE ONLINE (pg 127) "Explain some steps we can take to take care of our own and other people's safety and wellbeing when using social media." "Identify some ways in which we can recognise when we are being manipulated by online content or contact, and ways to respond."

		HEALTHY LIFESTYLES HL5 – BODY IMAGE (PG 138) "Identify some ways in which images of people may be manipulated in the media/social media and therefore not reflect reality." "Explain why advertisers might use manipulated images and how recognising this might influence our responses." THE WORLD I LIVE IN WILI2 – MANAGING ONLINE INFORMATION (PG 139) "Recognise that not everything we see online is 'real' or 'true'. "Recognise that advertising online is targeted at individuals." "Identify some of the techniques that advertisers might use to get our attention or persuade us to believe something is true, and what their motives might be."

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 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	SELF CARE SUPPORT AND SAFETY - SS4 KEEPING SAFE ONLINE (pg 127) "Explain some steps we can take to take care of our own and other people's safety and wellbeing when using social media." "Identify some ways in which we can recognise when we are being manipulated by online content or contact, and ways to respond." "Describe some ways in which social media can be used in a safe and positive way." "Explain how some behaviours on social media might damage friendships and relationships." "Identify sources of advice and support, and ways to report online concerns." HEALTHY LIFESTYLES – HL1 – ELEMENTS OF A HEALTHY LIFESTYLE (PG 136) "Describe what might affect choices we make about our health, e.g. healthy eating (advertising), physical activity (playing on the computer, restrictions due to health conditions) sleep (worries, stress, social media)."

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 or curated lives • How and why people are unkind or hurtful online when they would not necessarily be unkind to someone face to face	SELF CARE SUPPORT AND SAFETY - SS4 KEEPING SAFE ONLINE (pg 127) "Explain what is meant by social media and how people use social media." "Recognise that not all information seen online is true." "Explain how some behaviours on social media might damage friendships and relationships." "Explain some steps we can take to take care of our own and other people's safety and wellbeing when using social media." "Identify some ways in which we can recognise when we are being manipulated by online content or contact, and ways to respond." MANAGING FEELINGS MF1 – SELF ESTEEM AND UNKIND COMMENTS (PG130) "Demonstrate simple strategies to help manage our feelings about unhelpful/unkind comments." "Demonstrate polite and assertive ways of challenging unkind comments directed at us or others."

		HEALTHY LIFESTYLES HL5 – BODY IMAGE (PG 138) "Identify some ways in which images of people may be manipulated in the media/social media and therefore not reflect reality." THE WORLD I LIVE IN WILI2 – MANAGING ONLINE INFORMATION (PG 139) Recognise that not everything we see online is 'real' or 'true'.
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	SELF CARE SUPPORT AND SAFETY - SS4 KEEPING SAFE ONLINE (pg 127) "Describe some ways in which social media can be used in a safe and positive way." "Identify what we should do before we 'like', 'forward' or 'share' on social media and how this helps to keep us safe online." "Identify some possible risks of using social media." "Identify sources of advice and support, and ways to report online

		concerns." "Identify how to make safe, reliable choices from search results." SELF CARE SUPPORT AND SAFETY - SS6 PUBLIC AND PRIVATE (PG 128) "Explain and demonstrate how to ask for help and whom to go to if we have seen something upsetting or done something online that we are now worried about or regret."
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.	SELF CARE SUPPORT AND SAFETY - SS4 KEEPING SAFE ONLINE (pg 127) "Identify sources of advice and support, and ways to report online concerns." "Identify how to make safe, reliable choices from search results." "Explain some steps we can take to take care of our own and other people's safety and wellbeing when using social media." "Identify some ways in which we can recognise when we are being manipulated by online content or contact, and ways to respond." HEALTHY LIFESTYLES

		HL1 – ELEMENTS OF A HEALTHY LIFESTYLE (PG 136) “Describe what might affect choices we make about our health, e.g. healthy eating (advertising), physical activity (playing on the computer, restrictions due to health conditions) sleep (worries, stress, social media).” “Describe strategies for managing pressures and influences on healthy lifestyle choices.”