*Doing our best to achieve our best*

Clarendon Primary School

# Online Safety Policy

*This policy applies to all members of the school community (including staff, children, volunteers, parents/carers, visitors and community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).*

Date policy last reviewed: November 2024

**Contents:**

**Introduction and Overview**

At Clarendon Primary School, we are committed to ensuring the best safeguarding procedures are in place and see online safety as a high priority in ensuring the safety and welfare of our children. We aim to deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (e.g. mobile phones) in accordance with statutory guidance.

Online safety is integral to other school policies including the Behaviour Policy, Child Protection Policy and Anti-Bullying Policy. Clarendon Primary School will deal with incidents within this policy and associated behaviour and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

**Statement of intent**

Clarendon Primary School understands that using online services is an important aspect of raising educational standards, promoting pupil achievement, and enhancing teaching and learning. The use of online services is embedded throughout the school; therefore, there are a number of controls in place to ensure the safety of pupils and staff.

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

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

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

**The purpose of this policy is to:**

- Outline the guiding principles for all members of the school community regarding the use of ICT.
- Safeguard and protect pupils and staff and help them to work safely and responsibly with the internet and other communication technologies.
- Set clear expectations of behaviour relating to responsible use of the internet for educational, personal or recreational use.
- Establish clear reporting mechanisms to deal with online abuse such as bullying that are cross-referenced with other school policies.
- Ensure that all members of the school community know that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

## 1. Legal framework

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

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

This policy operates in conjunction with the following school policies:

- Technology Acceptable Use Agreement
- Cyber Response and Recovery Plan
- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- Staff Code of Conduct
- Behaviour Policy
- Disciplinary Policy and Procedure
- Data Protection Policy
- Confidentiality Policy
- Prevent Duty Risk Assessment

## 2. Roles and responsibilities

The governing board will be responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy on an **annual** basis.
- Ensuring their own knowledge of online safety issues is up-to-date.
- Ensuring all staff undergo safeguarding and child protection training, including online safety, at induction and at regular intervals.
- Ensuring that there are appropriate filtering and monitoring systems in place.
- Ensuring that the effectiveness of filtering and monitoring systems is reviewed at least annually in liaison with ICT staff and service providers.
- Ensuring that the SLT and other relevant staff have an awareness and understanding of the filtering and monitoring provisions in place, and manage them effectively and know how to escalate concerns when identified.
- Ensuring that all relevant school policies have an effective approach to planning for, and responding to, online challenges and hoaxes embedded within them.

**The 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.
- 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 Online Safety Lead and ICT technicians to conduct regular light-touch reviews of this policy.
- Working with the DSL and governing board to update this policy on an **annual** basis.

**The DSL will be responsible for:**

- Taking the overall lead responsibility for online safety in the school.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the Online Safety Lead, SENCO and ICT technicians.
- Ensuring online safety is recognised as part of the school's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensuring safeguarding is considered in the school's approach to remote learning.
- Establishing a procedure for reporting online safety incidents and inappropriate internet use, both by pupils and staff, and ensuring all members of the school community understand this procedure.
- Understanding the filtering and monitoring processes in place at the school.
- Ensuring that all safeguarding training given to staff includes an understanding of the expectations, roles and responsibilities in relation to filtering and monitoring systems at the school.
- 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 online safety lead and ICT technicians to conduct regular reviews of this policy.

**Eduthing ICT technicians will be responsible for:**

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher.
- Ensuring that the school's filtering and monitoring systems are updated as appropriate.
- Working with the online safely lead and headteacher to conduct regular reviews of this policy.

**All staff members will be responsible for:**

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

**Pupils will be responsible for:**

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

## 3. Managing online safety

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

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

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

- Staff and governors receive regular training and are signposted to further online training should they want to undertake it

- Staff receive regular updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum and designated lessons are taught using Project Evolve
- Assemblies are conducted at least termly on the topic of remaining safe online

**Handling online safety concerns**

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

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

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

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

Concerns regarding a staff member's online behaviour are reported to the headteacher, who decides on the best course of action in line with the relevant policies. 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 DSL, who investigates concerns with relevant staff members and manages concerns in accordance with relevant policies depending on their nature, e.g. the Behaviour Policy and Child Protection and Safeguarding Policy.

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

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

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

## 4. Cyberbullying

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

- Threatening, intimidating or upsetting text messages
- Threatening or embarrassing pictures and video clips sent via mobile phone cameras
- Silent or abusive phone calls or using the victim's phone to harass others, to make them think the victim is responsible
- Threatening or bullying emails, possibly sent using a pseudonym or someone else's name
- Unpleasant messages sent via instant messaging

- Unpleasant or defamatory information posted to blogs, personal websites and social networking sites, e.g. Facebook
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

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

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

## 5. Child-on-child sexual abuse and harassment

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

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

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

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

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

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

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

## 6. Grooming and exploitation

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

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

Due to the fact pupils are less likely to report grooming than other online offences, it is particularly important that staff understand the indicators of this type of abuse. The DSL will ensure that online

safety training covers online abuse, the importance of looking for signs of grooming, and what the signs of online grooming are, including:

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

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

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

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

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

**Radicalisation**

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

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty Risk Assessment. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised. Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Prevent Duty Policy.

## 7. Mental health

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

## 8. Online hoaxes and harmful online challenges

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

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

Where staff suspect there may be a harmful online challenge or online hoax circulating amongst pupils in the school, they will report this to the DSL immediately.

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

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL 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 and in line with the Child Protection and Safeguarding Policy.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, they will ensure that the challenge is directly addressed to the relevant pupils, e.g. those within a particular age range that is directly affected or individual pupils at risk where appropriate.

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

## 9. Cyber-crime

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

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

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

The DSL and headteacher will ensure that pupils are taught, throughout the curriculum, how to use technology safely, responsibly and lawfully.

## 10. 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. All staff will be made aware that pupils are at risk of abuse, by their peers and by adults, online as well as in person, and that, often, abuse will take place concurrently via online channels and in daily life.

## 11. Online safety and the curriculum

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

- Relationships and health education
- PSHE
- Computing

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

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

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

The online risks pupils may face online are always considered when developing the curriculum. The risks that are considered and how they are covered in the curriculum can be found in appendix A of this policy.

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

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

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

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

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

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

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

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

## 12. Use of technology in the classroom

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

- Computers
- Chromebooks
- Tablets
- 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 will review and evaluate the resource. Class teachers will ensure that any internet-derived materials are used in line with copyright law.

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

## 13. Use of smart technology

While the school recognises that the use of smart technology can have educational benefits, there are also a variety of associated risks which the school will ensure it manages.
Pupils will be educated on the acceptable and appropriate use of personal devices and will use technology in line with the school's Technology Acceptable Use Agreement for Pupils.
Staff will use all smart technology and personal technology in line with the school's policies.
The school recognises that pupils' unlimited and unrestricted access to the internet via mobile phone networks means that some pupils may use the internet in a way which breaches the school's acceptable use of ICT agreement for pupils.

Inappropriate use of smart technology may include:

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

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

Where it is deemed necessary, the school will ban pupil's use of personal technology whilst on school site.

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

The school will hold assemblies, where appropriate, which address any specific concerns related to the misuse of smart technology and outline the importance of using smart technology in an appropriate manner.

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

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

## 14. Educating parents

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

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

- Child sexual abuse, including grooming.

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

Parents will be informed of the ways in which they can prevent their child from accessing harmful content at home, e.g. by implementing parental controls to block age-inappropriate content.
Parental awareness regarding how they can support their children to be safe online will be raised in the following ways:

- Parents' evenings
- Twilight training sessions
- Newsletters
- Online resources

## 15. Internet access

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

## 16. Filtering and monitoring online activity

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

The 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 filtering and monitoring systems the school implements will be appropriate to pupils' ages, the number of pupils using the network, how often pupils access the network, and the proportionality of costs compared to the risks. ICT technicians and the Online Safety Lead will undertake regular checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system will be directed to Eduthing and approved by the Headteacher. Prior to making any changes to the filtering system, ICT technicians and the DSL will conduct a risk assessment. Any changes made to the system will be recorded by ICT technicians.

Reports of inappropriate websites or materials will be made to an ICT technician immediately, who will investigate the matter and makes any necessary changes.

Deliberate breaches of the filtering system will be reported to the DSL and ICT technicians, who will escalate the matter appropriately. If a pupil has deliberately breached the filtering system, they will be disciplined in line with the Behaviour Policy. If a member of staff has deliberately breached the filtering system, they will be disciplined in line with the Disciplinary Policy and Procedure.

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

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

## 17. Network security

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

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

All members of staff will have their own unique usernames and private passwords to access the school's systems. Pupils in Year 1 and above will be provided with their own unique username and private passwords. Staff members and pupils 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. Staff passwords will expire after **90** days, after which users will be required to change them.

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

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

## 18. Emails

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

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. Prior to being authorised to use the email system, staff must agree to and sign the Acceptable Use Agreement. Personal email accounts will not be permitted to be used on the school site. Any email that contains sensitive or personal information will only be sent using secure and encrypted email.

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

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

## 19. Generative artificial intelligence (AI)

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

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

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

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

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

## 20. Social networking

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

## 21. 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.
The website will be managed in line with the School Website Policy.

## 22. Use of devices

Staff members and pupils will be issued with school-owned devices to assist with their work, where necessary.

The use of personal devices on the school premises and for the purposes of school work must ensure that use complies with the school's Acceptable Use Agreement.

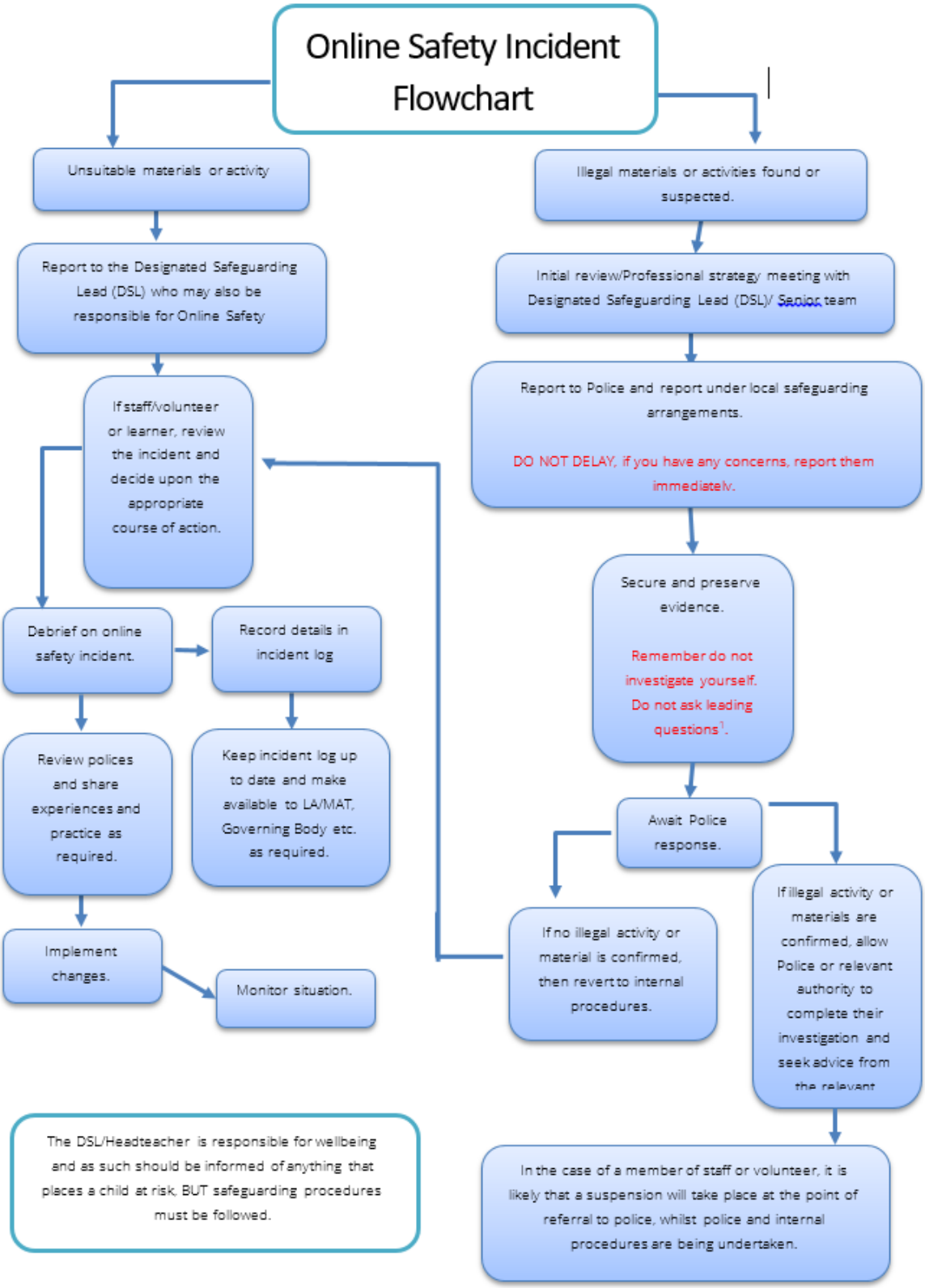
Staff must not store images of pupils or pupils personal data on any personal devices.

## 23. Remote learning

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

## 24. Monitoring and review

The school recognises that the online world is constantly changing; therefore, the DSL, ICT technicians and the Online Safety Lead conduct regular light-touch reviews of this policy to evaluate its effectiveness.
The governing board, headteacher and Online Safety Lead 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 **September 2025**.
Any changes made to this policy are communicated to all members of the school community.


Online Safety Incident Flowchart
Unsuitable materials or activity
Report to the Designated Safeguarding Lead (DSL) who may also be responsible for Online Safety
If staff/volunteer or learner, review the incident and decide upon the appropriate course of action.
Debrief on online safety incident.
Record details in incident log
Review polices and share experiences and practice as required.
Keep incident log up to date and make available to LA/MAT, Governing Body etc. as required.
Implement changes.
Monitor situation.
Illegal materials or activities found or suspected.
Initial review/Professional strategy meeting with Designated Safeguarding Lead (DSL)/ Senior team
Report to Police and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not ask leading questions[1].
Await Police response.
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.
The DSL/Headteacher is responsible for wellbeing and as such should be informed of anything that places a child at risk, BUT safeguarding procedures must be followed.

**Appendix 1**

# Online Safety Computing Curriculum Map

These lessons are planned using both Project Evolve and the SCARF PSHE curriculum.

| | Self-image & identity | Online Relationships | Online Reputation | Online Bullying | Managing Online Information | Health, Well-Being & Lifestyle | Privacy & Security | Copyright & Ownership |
|---|---|---|---|---|---|---|---|---|
| **EYFS** | I can recognise that I can say 'no', 'please stop', 'I'll tell', 'I'll ask' to somebody who asks me to do something that makes me feel sad, embarrassed or upset.<br><br>I can explain how this could be either in real life or online. | I can recognise some ways in which the internet can be used to communicate.<br><br>I can give examples of how (I might) use this technology to communicate with people I know. | I can identify ways that I can put information on the internet. | I can describe ways that some people can be unkind online.<br><br>I can offer examples of how this can make others feel. | I can talk about how I can use the internet to find things out.<br><br>I can identify devices I could use to access information on the internet.<br><br>I can give simple examples of how to find information (e.g. search engine, voice activated searching) | I can identify rules that help keep us safe and healthy in and beyond the home when using technology.<br><br>I can give some simple examples. | I can identify some simple examples of my personal information (e.g. name, address, birthday, age, location)<br><br>I can describe the people I can trust and can share this with; I can explain why I can trust them. | I know that the work I create belongs to me.<br>I can name my work so that others know it belongs to me. |
| **Year 1** | I can recognise that there may be people online who could make me feel sad, embarrassed or upset.<br><br>If something happens that makes me feel sad, worried, uncomfortable or frightened I can give examples of when and how to speak to an adult I can trust. | I can use the internet with adult support to communicate with people I know.<br><br>I can explain why it is important to be considerate and kind to people online. | I can recognise that information can stay online and could be copied.<br><br>I can describe what information I should not put online without asking a trusted adult first. | I can describe how to behave online in ways that do not upset others and can give examples. | I can use the internet to find things out.<br><br>I can use simple keywords in search engines.<br><br>I can describe and demonstrate how to get help from a trusted adult or helpline if I find content that makes me feel sad, uncomfortable, worried or frightened. | I can explain rules to keep us safe when we are using technology both in and beyond home.<br><br>I can give examples of some of these rules. | I can recognise more detailed examples of information that is personal to me (e.g. where I live, my family's names, where I go to school).<br><br>I can explain why I should always ask a trusted adult before I share any information about myself online.<br><br>I can explain why passwords can be used to protect information and devices. | I can explain why the work I create using technology belongs to me.<br><br>I can say why it belongs to me (e.g. "It is my idea" / "I designed it")<br><br>I can save my work so that others know it belongs to me (e.g. filename, name on content) |
| **Year 2** | I can explain how other people's identities online can be different to their identity in real life.<br><br>I can describe ways in which people might make themselves look different online.<br><br>I can give examples of online issues that might make me feel sad, worried, uncomfortable or frightened. I can give examples of how I might get help. | I can use the internet to communicate with people I don't know well (e.g. email a penpal in another school/country).<br><br>I can give examples of how I might use technology to communicate with others I don't know well. | I can explain how information put online about me can last for a long time.<br><br>I know who to talk to if I think someone has made a mistake about putting something online. | I can give examples of bullying behaviour and how it could look online.<br><br>I understand how bullying can make someone feel.<br><br>I can talk about how someone can/would get help about being bullied online or offline. | I can use keywords in search engines.<br><br>I can demonstrate how to navigate a simple webpage to get information I need (e.g. home, forward, back buttons; links, tabs and sections)<br><br>I can explain what voice activated searching is and how it might be used (e.g. Alexa, Google Now, iri).<br><br>I can explain the difference between things that are imaginary, 'made up', or 'make believe' and things that are 'true' or 'real'.<br><br>I can explain why some information I find online may not be true. | I can explain simple guidance for using technology in different environments and settings.<br><br>I can say how those rules/guides can help me. | I can describe and explain some rules for keeping my information private.<br><br>I can explain what passwords are and can use passwords for my accounts and devices.<br><br>I can explain how many devices in my home could be connected to the internet and can list some of those devices. | I can describe why other people's work belongs to them.<br><br>I can recognise that content on the internet may belong to other people. |
| **Year 3** | I can explain what is meant by the term 'identity'.<br><br>I can explain how I can represent myself in different ways online.<br><br>I can explain ways in which and why I might change my identity online depending on what I am doing online. | I can describe ways people who have similar likes and interests can get together online.<br><br>I can explain some risks of communicating online with others I don't know well.<br><br>I can explain what it means to 'know someone' online and why this may be different from knowing them in real life.<br><br>I can explain why I should be careful who I trust online and what information I trust them with.<br><br>I can explain what is meant by 'trusting someone online' and I can explain why this is different to 'liking someone online' | I can explain how to search for information about others online.<br><br>I can recognise I need to be careful before I share anything about myself or others online.<br><br>I know who I should ask if I am not sure if I should put something online. | I can explain what bullying is and can describe how people may bully others.<br><br>I can describe rules about how to behave online and how I follow them. | I can use key phrases in search engines.<br><br>I can explain the difference between a belief, an opinion and a fact. | I can explain why spending too much time using technology can sometimes have a negative impact on me; I can give some examples of activities where it is easy to spend a lot of time engaged (e.g. games, films, videos). | I can give reasons why I should only share information with people I choose to and can trust. I can explain that if I am not sure or feel pressured I should ask a trusted adult.<br><br>I can understand and can give reasons why passwords are important.<br><br>I can describe simple strategies for creating and keeping passwords private.<br><br>I can describe how connected devices can collect and share my information with others. | I can explain why copying someone else's work from the internet without permission can cause problems.<br><br>I can give examples of what these problems might be. |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | I can explain why I can take back my trust in someone or something if I feel nervous, uncomfortable or worried. | | | | | | |
| **Year 4** | I can explain how my online identity can be different to the identity I present in real life.<br><br>Knowing this, I can describe the right decisions about how I interact with others and how others perceive me. | I can give examples of how to be respectful to others online. | I can describe how others can find out information about me by looking online.<br><br>I can explain ways that some of the information about me online could have been created, copied or shared by others. | I can describe ways people can be bullied through a range of media (e.g. image, video, text, chat).<br><br>I can identify some online technologies where bullying might take place.<br><br>I can explain why I need to think carefully about how content I post might affect others, their feelings and how it may affect how others feel about them (their reputation). | I can describe how I can search for information within a wide group of technologies (e.g. social media, image sites, video sites).<br><br>I can describe some of the methods used to encourage people to buy things online (e.g. advertising offers; in-app purchases; pop-ups) and can recognise some of these when they appear.<br><br>I can explain that some people I 'meet online' may be computer programmes pretending to be real people. | I can explain how using technology can distract me from other things I might do or should be doing.<br><br>I can identify times or situations when I might need to limit the amount of time I use technology and suggest strategies to help me with this. | I can explain what a strong password is and describe strategies for keeping my personal information private, depending on context.<br><br>I can explain that internet use is never fully private and is monitored e.g. adult supervision. | When searching on the internet for content to use, I can explain why I need to consider who owns it and whether I have the right to reuse it.<br><br>I can give some simple examples. |
| **Year 5** | I can explain how identity online can be copied, modified or altered.<br><br>I can demonstrate responsible choices about my online identity; depending on context. | I can explain that there are some people who I communicate with online who may want to do me or my friends harm. I can recognise that this is not my/our fault.<br><br>I can make positive contributions and be part of online communities.<br><br>I can describe some of the communities in which I am involved and describe how I collaborate with others positively. | I can search for information about an individual online and create a summary report of the information I find.<br><br>I can describe ways that information about people online can be used by others to make judgements about an individual. | I can recognise when someone is upset, hurt or angry online.<br><br>I can describe how to get help for someone that is being bullied online and assess when I need to do or say something or tell someone.<br><br>I can explain how I would report online bullying on the apps and platforms that I use.<br><br>I can describe the helpline services who can support me and what I would say and do if I needed their help e.g. Childline.<br><br>I can explain how to block abusive users. | I can explain what is meant by 'being sceptical'. I can give some examples of when and why it is important to be sceptical.<br><br>I can explain what is meant by a hoax. I can explain why I need to think carefully before I forward anything online.<br><br>I can explain why some information I find online may not be honest, accurate or legal.<br><br>I can explain why information that is on a large number of sites may still be inaccurate or untrue. I can assess how this might happen (accident or on purpose) | I can describe ways technology can affect healthy sleep and can describe some of the issues.<br><br>I can describe some strategies, tips or advice to promote healthy sleep with regards to technology. | I can create and use strong and secure passwords.<br><br>I can explain how many free apps or services may read and share my private information (e.g. friends, contacts, likes, images, videos, voice messages, geolocation) with others.<br><br>I can explain how and why some apps may request or take payment for additional content (e.g. in-app purchases) and explain why I should seek permission from a trusted adult before purchasing. | I can assess and justify when it is acceptable to use the work of others.<br><br>I can give examples of content that is permitted to be reused. |
| **Year 6** | I can describe ways in which the media can shape ideas about gender.<br><br>I can identify messages about gender roles and make judgements based on them.<br><br>I can challenge and explain why it is important to reject inappropriate messages about gender online.<br><br>I can describe issues online that might make me or others feel sad, worried, uncomfortable or frightened. I know and can give examples of how I might get help, both on and offline.<br><br>I can explain why I should keep asking until I get the help I need. | I can explain how sharing something online may have an impact either positively or negatively<br><br>I can describe how things shared privately online can have unintended consequences for others e.g. screen grab.<br><br>I can explain that taking/sharing inappropriate images of someone may have an impact for the sharer and others; and who can help if someone is worried about this. | I can explain how I am developing an online reputation which will allow other people to form an opinion of me.<br><br>I can describe some simple ways that help build a positive online reputation. | I can describe how to capture bullying content as evidence (e.g. screen grab, URL, profile) to share with others who can help me.<br><br>I can explain how someone could report online bullying in different contexts. | I can explain how search engines work and how results are selected and ranked.<br><br>I can demonstrate the strategies I would apply to be discerning in evaluating digital content.<br><br>I can describe how some online information can be opinion and can offer examples.<br><br>I can define the terms 'influence', 'manipulation' and 'persuasion' and explain how I might encounter these online e.g. advertising and ad-targeting.<br><br>I can explain how and why some people may present opinions as facts.<br><br>I can demonstrate strategies to enable me to analyse and evaluate the validity of facts and I can explain why using these strategies are important.<br><br>I can identify and flag inappropriate content. | I recognise and can discuss the pressures that technology can place on someone and how/when they could manage this.<br><br>I can recognise features of persuasive design and how they are used to keep users engaged (current and future use)<br><br>I can assess and action different strategies to limit the impact of technology on my health (e.g. night-shift mode, regular breaks, correct posture, sleep, diet and exercise). | I can describe effective strategies for managing those passwords.<br>I know what to do if my password is lost or stolen.<br><br>I can describe ways in which some online content targets people to gain money or information illegally;<br><br>I can describe strategies to help me identify such content (e.g. scams, phishing). | I can demonstrate the use of search tools to find and access online content which can be reused by others.<br><br>I can demonstrate how to make references to and acknowledge sources I have used from the internet. |