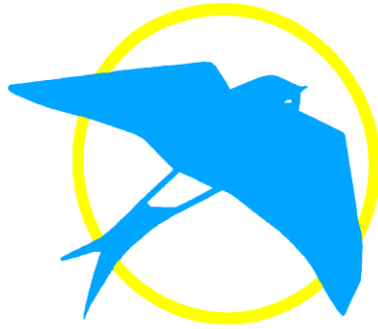




Martin Primary School

Online Safety Policy

Reviewed and ratified by the Governing Body: autumn 2026

Reviewed every year

Statement of intent

Martin 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, self-harm and suicide, racism, misogyny, anti-Semitism, radicalisation, extreme sexual or physical violence, misinformation, disinformation (including fake news), conspiracy theories and discriminatory or extremist views.
- **Contact:** Being subjected to harmful online interaction with other users or generative AI applications that simulate this, e.g. peer pressure, commercial advertising, and adults posing as children or young adults with the intention to groom or exploit children for sexual, criminal, financial or other purposes.
- **Conduct:** Personal online behaviour that increases the likelihood of, or causes, harm, e.g. making, sending and receiving explicit messages and images including those generated using AI, 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:

- Online Safety Act 2023
- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Data (Use and Access) Act 2025
- Children's wellbeing and schools Act 2026
- DfE (2024) 'Filtering and monitoring standards for schools and colleges'
- DfE (2021) 'Harmful online challenges and online hoaxes'
- DfE (2026) 'Keeping children safe in education 2026'
- DfE (2019) 'Teaching online safety in school'
- DfE (2018) 'Searching, screening and confiscation'
- Department for Science, Innovation and Technology and UK Council for Internet Safety (2024) 'Sharing nudes and semi-nudes: advice for education settings working with children and young people'
- UK Council for Child Internet Safety (2020) 'Education for a Connected World – 2020 edition'
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'

This policy operates in conjunction with the following school policies:

- Allegations of Abuse Against Staff Policy
- Low-level Safeguarding Concerns Policy
- Acceptable Use Agreement
- Child Protection and Safeguarding Policy
- Anti-Bullying Policy
- PSHE Policy
- Staff Code of Conduct
- Behaviour Policy
- Data Protection Policy
- Confidentiality Policy
- AI Policy

This policy links with the UN Rights of the Child:

Article 13

Every child must be free to say what they think and to seek and receive all kinds of information, as long as it is within the law.

Article 17

Every child has the right to reliable information from the media. This should be information that children can understand. Governments must help protect children from materials that could harm them.

2. Roles and responsibilities

Designated Safeguarding team	Hannah Taylor Ziz Chater Chantal Lust Shona Glackin
Online safety team	Hannah Taylor Chantal Lust Jess Lundie Neng Chong
Online safety / safeguarding link governor	Gabrielle Sharpe
Technical support	Neng Chong

The Governing Body is responsible for:

- Ensuring that this policy is effective and complies with relevant laws and statutory guidance.
- Ensuring the DSL's remit covers online safety.
- Reviewing this policy 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 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.
- Ensuring compliance with the DfE's 'Meeting digital and technology standards in schools and colleges', with particular regard to the filtering and monitoring standards in relation to safeguarding.

The headteacher 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 DSL and Governing Body to update this policy on an annual basis.
- Identifying and assigning roles and responsibilities to manage the school's filtering and monitoring systems.
- Appointing an SLT digital lead in line with the Cyber-security Policy.

The DSL is responsible for:

- Taking the lead responsibility for online safety in the school.
- Acting as the named point of contact within the school on all online safeguarding issues.
- Undertaking training so they understand the risks associated with online safety and can recognise additional risks that pupils with SEND face online.
- Liaising with relevant members of staff on online safety matters, e.g. the SENCO and The ICT technician.
- 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.
- Working closely with the police during police investigations.
- 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 and ensuring all members of the school community understand the reporting 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 detailed, secure and accurate written records of reported online safety concerns as well as the decisions and whether or not referrals have been made.
- Understanding the purpose of record keeping.
- 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.
- Working with the headteacher and Governing Body to update this policy on an annual basis.

The ICT technician is responsible for:

- Providing technical support in the development and implementation of the school's online safety policies and procedures.
- Implementing appropriate security measures as directed by the headteacher.
- 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 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 receive regular email updates regarding online safety information and any changes to online safety guidance or legislation
- Online safety is integrated into learning throughout the curriculum
- Assemblies for children in Year 5 and Year 6 are conducted 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 pupils may not feel ready or know how to tell someone about abuse they are experiencing, due to feeling embarrassed, humiliated, or threatened. Staff will be aware and recognise the importance of the presence and scale of online abuse or harassment, by considering that just because it is not being reported, does not mean it is not happening.

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 and appropriate support provided to the victim.

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 DSL, who investigates concerns with relevant staff members, e.g. the headteacher and The ICT

technician, 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
- Abuse between young people in intimate relationships online i.e. teenage relationship abuse
- Discriminatory bullying online i.e. homophobia, racism, misogyny/misandry.

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

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

5. Child-on-child sexual abuse and harassment

All staff will be aware of the indicators of abuse, neglect and exploitation and understand where the risk of such harms can occur online. 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 including those generated or altered using AI
- Abuse between young people in intimate relationships online, i.e. teenage relationship abuse

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

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

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

The school responds 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 are 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.
- Having an older boyfriend or girlfriend, usually one that does not attend the school and whom their close friends have not met.

- Having money or new possessions, e.g. clothes and technological devices, that they cannot or will not explain.

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

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

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

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

Radicalisation

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

Staff members will be aware of the factors which can place certain pupils at increased vulnerability to radicalisation, as outlined in the Prevent Duty Policy. Staff will be expected to exercise vigilance towards any pupils displaying indicators that they have been, or are being, radicalised.

Where staff have a concern about a pupil relating to radicalisation, they will report this to the DSL without delay, who will handle the situation in line with the Prevent Duty Policy.

7. Mental health

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

8. Online hoaxes and harmful online challenges

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

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

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

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

Prior to deciding how to respond to a harmful online challenge or hoax, the DSL and the headteacher will decide whether each proposed response is:

- In line with any advice received from a known, reliable source, e.g. the UK Safer Internet Centre, when fact-checking the risk of online challenges or hoaxes.
- Careful to avoid needlessly scaring or distressing pupils.
- Not inadvertently encouraging pupils to view the hoax or challenge where they would not have otherwise come across it, e.g. where content is explained to younger pupils but is almost exclusively being shared amongst older pupils.
- Proportional to the actual or perceived risk.
- Helpful to the pupils who are, or are perceived to be, at risk.
- Appropriate for the relevant pupils' age and developmental stage.
- Supportive.
- In line with the Child Protection and Safeguarding Policy.

Where the DSL's assessment finds an online challenge to be putting pupils at risk of harm, 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 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, 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, 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.

Staff training will include a specific focus on harmful online narratives such as misinformation, disinformation, and conspiracy theories, helping staff to recognise the signs of influence or vulnerability among pupils.

Training will equip staff with the knowledge and confidence to identify signs of online harm, respond appropriately to disclosures or concerns, and support pupils in developing critical thinking skills and safe online behaviours.

Staff will also be guided on how to embed online safety themes across the wider curriculum, promoting a consistent, whole-school approach to digital safeguarding.

Information about the school's full responses to online safeguarding incidents can be found in the Anti-bullying Policy, the Child-on-child Abuse Policy and the Child Protection and Safeguarding Policy.

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

- ICT

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

The school's approach to teaching online safety in the curriculum will reflect the ever-evolving nature of online risks, ensuring pupils develop the knowledge and resilience to navigate digital spaces safely and responsibly. Online safety education will address four key categories of risk: content, contact, conduct, and commerce.

Content risks

Pupils will be taught how to critically evaluate online content and identify material that is illegal, inappropriate, or harmful. The curriculum will include discussions around harmful content such as AI-generated content, deepfakes, pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news), and conspiracy theories. Lessons will equip pupils with the skills to question sources, verify information, and understand the dangers of engaging with such content.

Contact risks

The school will educate pupils about the potential dangers of interacting with others online or generative AI applications that simulate this. Pupils will explore topics such as peer pressure, commercial exploitation, and grooming tactics used by adults who pose as children or young adults. They will learn how to recognise unsafe interactions, use privacy settings effectively, and report any concerning behaviour or messages to trusted adults and platforms.

Conduct risks

Pupils will be guided on how their own online behaviour can impact both themselves and others. The curriculum will address the risks associated with making, sharing or receiving nudes and semi-nudes, including images that have been generated or altered using AI. Online bullying, including the use online platforms, e.g. social media and messaging platforms to harass or intimidate others, will also be a key focus. Pupils will be taught responsible digital conduct and the legal and emotional consequences of harmful behaviour.

Commerce risks

The curriculum will also include education on online commercial risks. Pupils will be informed about the dangers of online gambling, exposure to inappropriate advertising, and financial scams such as phishing. They will learn how to recognise fraudulent schemes, protect their personal and financial information, and seek help when confronted with suspicious online activity.

The school follows the [Project Evolve](#) curriculum for online safety. 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 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 1 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 SENCO 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.

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 and DSL 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 advises the staff member on how to best support any pupil who may be especially impacted by a lesson or activity. 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:

- Computers
- Laptops
- Tablets
- Chromebooks
- Ipad

Prior to using any websites, tools, apps, AI systems 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 mobile devices

Pupils

Pupils are not permitted to use mobile devices or any other personal technology whilst in school.

Pupils are not permitted to bring Smartphones or any device that has online access, apps, cameras or audio/video recording to school. Independent travellers can bring 'text and talk only' mobile phones to school but they must be switched off and handed to the class teacher on arrival and collected when the pupil leaves. Any unauthorised device, or any device used during the school day, will be confiscated in line with the school's Behaviour Policy.

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.

Staff

Any personal electronic device that is brought into school is the responsibility of the user. Staff members are not permitted to use their personal devices in the presence of children except when on educational visits for safeguarding purposes. Staff are only permitted to take photos using their personal devices with the express permission of the headteacher and when another member of staff is present. This must not include photos of any children (see point 25 below).

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.

Any concerns about visitors' use of personal devices on the school premises are reported to the DSL.

14. Educating parents

The 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 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.
- Making or sharing nudes and semi-nudes, including images generated or altered using AI.
- 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:

- Parent information meetings
- Distributing monthly newsletters from Knowsley Online Safety Learning Centre

15. Internet access

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

16. Filtering and monitoring online activity

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

The school will do all it reasonably can to limit pupils' exposure to online risks from the school's ICT system. The school will put in place appropriate filtering and monitoring systems and ensure that their effectiveness is reviewed at least annually and whenever there is a significant change to the school's network, safeguarding risks or

technology provision. Reviews will be carried out by the SLT member responsible for filtering and monitoring with support from the DSL and ICT technicians.

Reviews will include checks that filtering is working appropriately on all internet-connected devices in all relevant locations, and a record will be kept of these checks.

At this school, the internet connection is provided by LGfL. This means there is a dedicated and secure, schoolsafe connection that is protected with firewalls and multiple layers of security, including a web filtering system called WebScreen 3, which is made specifically to protect children in schools.

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

The headteacher and ICT technicians will undertake an audit to determine what filtering and monitoring systems are required. The filtering and monitoring systems the school implements are 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. The ICT technician undertakes termly checks on the filtering and monitoring systems to ensure they are effective and appropriate.

Requests regarding making changes to the filtering system are directed to the headteacher. Prior to making any changes to the filtering system, the ICT technician and the DSL conduct a risk assessment. Any changes made to the system are recorded by the ICT technician. Reports of inappropriate websites or materials are made to an ICT technician immediately, who investigates the matter and makes any necessary changes.

Deliberate breaches of the filtering system are reported to the DSL and The ICT technician, 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 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 Child Protection and Safeguarding Policy.

17. Network security

Technical security features, such as anti-virus software, are kept up-to-date and are switched on at all times.

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 ICT technician.

All members of staff have their own unique usernames and private passwords to access the school's systems. Staff members 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. Passwords expire after 90 days, after which users are required to change them.

Users inform The ICT technician 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 and Cyber-security Breach Prevention and Management Plan.

18. Emails

Staff at this school use the StaffMail system for all school emails. This system is linked to the USO authentication system and is fully auditable, trackable and managed by LGfL on behalf of the school. This is for the mutual protection and privacy of all staff, pupils and parents/carers, as well as to support data protection. Access to and the use of emails is managed in line with the Data Protection Policy and Acceptable Use Agreement.

Staff 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 must agree to and sign the Acceptable Use Agreement. Any email that contains sensitive or personal information is only sent using secure and encrypted email.

Staff members are required to block spam and junk mail, and report the matter to The ICT technician. 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. SLT will organise **annual** cyber awareness training, including guidance on recognising phishing emails, AI-generated phishing attempts and other malicious communications. This training will include information on the following:

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

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

19. Generative artificial intelligence (AI) - see also AI Policy

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, confidential and sensitive data is not entered into generative AI tools unless this is authorised, secure and compliant with data protection legislation.

Where staff use AI tools to support teaching, learning or administrative tasks, they will do so in accordance with the school's AI Policy and DfE guidance on generative AI in education.

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

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 can use personal social media during break and lunchtimes when there are no children present; however, inappropriate or excessive use of personal social media during school hours may result in the removal of internet access or further action. 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 follow these expectations at all times.

Staff are only permitted to communicate with pupils or parents over social networking sites for school business purposes with the permission of the headteacher 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 a parent at the school or are friends with a parent at the school, they 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 Policy.

21. 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 the appropriate permissions have been obtained.

22. Google Drive

This school adheres to the principles of the DfE document '[Cloud computing services: guidance for school leaders, school staff and governing bodies](#)'. The data protection officer and technical support analyse and document systems and procedures before they are implemented, and regularly review them.

The following principles apply:

- the DPO approves new cloud systems, what may or may not be stored in them and by whom. This is noted in a DPIA (data-protection impact statement) and parental permission is sought
- regular training ensures all staff understand sharing functionality and this is audited to ensure that pupil data is not shared by mistake. Open access or widely shared folders are clearly marked as such
- pupils and staff are only given access and/or sharing rights when they can demonstrate an understanding of what data may be stored and how it can be seen
- two-factor authentication is used for access to staff or pupil data will be used when possible and as it can be implemented in to school systems.
- only school-approved platforms are used by staff to store pupil work
- all stakeholders understand the difference between consumer and education products (e.g. a private Gmail account or Google Drive and those belonging to a managed educational domain).

23. Use of school-owned devices

Staff members are issued with laptops to assist with their work, where necessary. Pupils are provided with school-owned devices as necessary to assist in the delivery of the curriculum, e.g. chromebooks to use during lessons.

Staff and pupils are not permitted to connect school-owned devices to public Wi-Fi networks. 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.

The ICT technician reviews all school-owned devices on a monthly basis to carry out software updates and ensure there is no inappropriate material or malware on the devices. No software, apps or other programmes can be downloaded onto a device without authorisation from The ICT technician.

Cases of staff members or pupils found to be misusing school-owned devices will be managed in line with the Disciplinary Policy and Procedure and Behaviour Policy respectively.

24. Remote learning

All remote learning is delivered in line with the school's 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.

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.

25. Digital images and video

The school imposes a range of restrictions as to what the school digitally records and publishes: all employees and governors are subject to these restrictions.

No photographs, videos, or digital images of children or adults are permitted to be taken at Martin Primary. The three exceptions to this are: 'Tapestry', which is covered under a separate agreement, photos for the school website (for which explicit permission must be obtained – see below), and official school photographs of individuals and classes.

Children's work can be photographed and this may include the child's hands, or other unidentifiable body part. This work will be labelled with the child's name. These images may also be stored e.g. for reference purposes.

Any events where pupils are performing will not be digitally recorded by the school e.g. Christmas show, Carol Concert, end of Y6 Leavers' show. This includes events on the school premises as well as those at other locations e.g. East Finchley Arts Festival. The school will take every precaution to minimise the chance of other bodies e.g. the

local press from taking photographs. However, this cannot be guaranteed in public places, as the school does not have ultimate jurisdiction in this setting.

Parents/carers/carers will be reminded that any images they take are for personal use only and are not to be shared via social media – attention will be drawn to the safeguarding implications.

If photos are required for the school's website, explicit written permission will be sought from individual parents/carers/carers. These photos will be carefully stage-managed and no 'background' children will be permitted. This process will be subjected to audit by non-staff members of the Governing Body, normally the designated safeguarding governor.

All outside providers where Martin Primary children are involved e.g. after school clubs etc... will be advised of these protocols and will be subject to them. This includes the Forest School and MHSA events for both children and adults e.g. Christmas Fair, Summer Fair, Quiz night, and so on. This list is just for illustrative purposes and is not exhaustive

The parents/carers/carers of children who have a medical condition will be asked to provide a colour photograph, signed on the back, to be displayed where necessary in the school in order to keep their child safe e.g. dining hall, staff room, school office.

Pupils are advised to be very careful about placing any personal photos on social media. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Pupils are taught that they should not post images or videos of others without their permission. The school teaches them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location. We teach them about the need to keep their data secure and what to do if they / or a friend are subject to bullying or abuse.

Martin Primary Online Safety Overview

	Autumn 1	Autumn 2	Spring 1	Spring 2	Summer 1	Summer 2
Year 1	Passwords and personal details	Benefits of the internet	What is trustworthy on the internet?		How to keep safe when using the internet	
Year 2	What is true and untrue online?	Rules and restrictions online	Who can you trust online?	Screen time and healthy habits	What to do if I feel unsafe online?	
Year 3	Appropriate and inappropriate behaviour online	Knowing the difference between: fact, opinion and a belief	Social media and what it is used for and age restrictions	Peer pressure online	Appropriate and inappropriate sources online	
Year 4	Online regulations and restrictions	Keeping private information and media safe online	Positive and negative distractions of technology		Recognising and managing risks online	
Year 5	Keeping personal information private online	Healthy habits online	Online bullying		Strategies for staying safe online	
Year 6	Consent online	Positive and negatives of online sharing	Healthy habits and screen time	Social media campaigns	Online bullying	

Key Stage 1: Acceptable Use Agreement

I keep **SAFE online** because ...



I **CHECK** it's OK to use a website / game / app.

I **ASK** for help if I get lost online.

I **THINK** before I click on things.

I **KNOW** online people are really strangers.

I am **RESPONSIBLE** so never share private information.

I am **KIND** and polite online.

I **TELL** a trusted adult if I am worried about anything.

My trusted adults are:

Mum

Dad

Teacher

My name:

Date signed:

--

KS2 Pupil Online Acceptable Use Agreement

This agreement will help keep me safe and help me to be fair to others.

- ***I am an online digital learner*** – I use the school's IT for schoolwork, homework and other activities approved by trusted adults.
- ***I am a secure online learner*** - I keep my logins and passwords secret.
- ***I am careful online*** - I think before I click on links and only download when I know it is safe or has been agreed by trusted adults.
- ***I am guarded online*** - I only give out my full home address, phone number or other personal information that could be used to identify me or my family and friends when my trusted adults have agreed.
- ***I am cautious online*** - I know that some websites and social networks have age restrictions and I respect this and I only visit internet sites that I know my trusted adults have agreed.
- ***I am considerate online*** - I do not get involved with bullying or sharing inappropriate material.
- ***I am respectful online*** – I do not respond to unkind or hurtful messages/comments and tell my trusted adults if I receive these.
- ***I am responsible online*** – I keep others safe by talking to my trusted adults if a friend or person I know is being bullied or harassed online or is being affected by things they see or hear online.
- ***I am a creative digital learner online*** - I only edit or delete my own digital work and only use other people's work with their permission or where the work is shared through a Creative Commons licence.
- ***I am a researcher online*** - I use safer search tools approved by my trusted adults and know to 'double check' all information I find online.
- ***I communicate and collaborate online*** - with people I know and have met in real life or that a trusted adult has approved.
- ***I am SMART online*** - I understand that unless I have met people in real life, an online person is actually a stranger. I may sometimes want to meet these strangers so I will always ask my trusted adults for advice.

I have read and understood this agreement. I know who are my trusted adults are and agree to the above.

Signed: _____ **Date:** _____