Reviewed: October 2026
Next Review Date: October 2027

Signed by:
Headteacher
Mrs Claire Jones
Date: October 2026

Co-Chairs of Governors
Mrs Joanna Potter and Mrs Danielle Smith
Date: October 2026

Euxton Primrose Hill Primary School

Online Safety Policy

Courage • Ambition • Respect • Excellence

Together we will make a difference

Statement of intent

Euxton Primrose Hill Primary School recognises that the safe and effective use of digital technology and online services is an important part of education. Technology can enhance teaching and learning, support communication and provide pupils with valuable opportunities to develop the knowledge and skills they need to participate safely and confidently in an increasingly digital world.

The school is committed to ensuring that pupils, staff, governors, volunteers and visitors understand how to use technology safely, responsibly and appropriately. Online safety is an integral part of our safeguarding responsibilities and is embedded within our curriculum, policies, procedures and daily practice.

We recognise that online risks are constantly evolving and that children may encounter harmful content or behaviour both in and outside school. We will work in partnership with parents and carers, staff, governors and relevant external agencies to promote online safety, respond effectively to concerns and support children who may be at increased risk of harm. All online safety concerns will be taken seriously, reported promptly and managed in accordance with the school's safeguarding procedures.

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

- **Content:** Being exposed to illegal, inappropriate or harmful material, including pornography, misinformation, disinformation, conspiracy theories, self-harm content and discriminatory or extremist views.
- **Contact:** Experiencing harmful interactions with other users, including grooming, exploitation, unwanted contact, peer pressure and manipulation by adults or other children.
- **Conduct:** Personal online behaviour that causes or increases the likelihood of harm, including online bullying, harassment, sharing intimate images and creating or sharing harmful content.
- **Commerce:** Risks associated with online financial activity, including scams, phishing, fraud, inappropriate advertising and online gambling.

These categories inform our approach to prevention, education, filtering and monitoring, and the management of online safety concerns.

This policy sets out the expectations and procedures that support the safe, responsible and age-appropriate use of the internet, digital devices and online services across the school community. It should be read alongside the school's other safeguarding and related policies.

Legal framework

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

Legislation

- Children Act 1989 and Children Act 2004.
- Education Act 2002.
- Equality Act 2010.
- Data Protection Act 2018 and UK General Data Protection Regulation (UK GDPR).
- Human Rights Act 1998.
- Computer Misuse Act 1990.
- Protection of Children Act 1978.
- Voyeurism (Offences) Act 2019.
- Online Safety Act 2023.

Statutory guidance and relevant guidance

This policy has regard to the following statutory and non-statutory guidance, as applicable and as amended or replaced:

- Department for Education, *Keeping Children Safe in Education* (2026).
- Department for Education, *Working Together to Safeguard Children* (2026).
- Department for Education, *Meeting digital and technology standards in schools and colleges*, including the filtering and monitoring and cyber security standards.
- Department for Education, *Teaching online safety in schools* (updated January 2023).
- Department for Education, *Searching, screening and confiscation: advice for schools* (updated July 2023).
- Department for Education, *Generative artificial intelligence (AI) in education* guidance.
- Department for Education and relevant safeguarding partners, *Sharing nudes and semi-nudes: advice for education settings working with children and young people*, using the current version.
- UK Council for Internet Safety, *Education for a Connected World*, using the current version.

Related school policies and agreements

This policy should be read alongside the school's relevant policies, procedures and agreements, including:

- Child Protection and Safeguarding Policy
- Staff Code of Conduct
- Behaviour Policy
- Data Protection Policy
- Cyber Security Policy.
- Prevent Policy
- Acceptable Use Agreements for staff and pupils

Roles and responsibilities

The governing board will be responsible for:

- Ensuring that this policy is implemented effectively, reviewed annually and updated when necessary to reflect changes in legislation, statutory guidance, technology and safeguarding practice.
- Ensuring that online safety is recognised as an integral part of the school's safeguarding responsibilities.
- Ensuring that the DSL has the appropriate knowledge, training, time and resources to fulfil their online safety responsibilities.
- Ensuring that appropriate filtering and monitoring systems are in place to safeguard pupils and staff.
- Ensuring that the effectiveness of filtering and monitoring arrangements is reviewed at least annually, with the headteacher, DSL and relevant ICT personnel or service providers.
- Ensuring that the school's approach to filtering and monitoring has clearly defined responsibilities for reviewing alerts, responding to concerns and escalating safeguarding issues.
- Ensuring that governors receive appropriate information and training to understand online safety risks and their safeguarding responsibilities.
- Ensuring that online safety is embedded within relevant school policies, safeguarding procedures and curriculum planning.
- Holding school leaders to account for the effective implementation of this policy and the school's online safety arrangements.

The Headteacher and Computing Subject Leader/Assistant Headteacher will be responsible for:

- Having overall responsibility for the school's online safety arrangements, including the effectiveness of filtering and monitoring systems.
- Ensuring that filtering and monitoring alerts and concerns are reviewed appropriately, with clear arrangements for responding to and escalating safeguarding concerns.
- Working with the ICT technician and relevant service providers to ensure that technical issues, weaknesses or failures affecting filtering, monitoring or network security are addressed promptly.
- Reviewing online safety arrangements regularly and following significant incidents, changes in technology or identified risks.
- Ensuring that relevant actions are recorded and that online safety concerns are managed in accordance with the school's safeguarding procedures.

The ICT technician will support these arrangements by maintaining the technical systems, carrying out agreed technical checks and reporting any identified weaknesses, failures or concerns to the Headteacher and Computing Subject Leader/Assistant Headteacher without delay.

The DSL will be responsible for:

- Taking the lead responsibility for online safety as part of the school's wider safeguarding arrangements.
- Ensuring that online safety concerns are recognised, reported, recorded and managed in accordance with the Child Protection and Safeguarding Policy.
- Ensuring that staff understand how to report online safety concerns involving pupils, other children, adults or members of staff.
- Ensuring that safeguarding concerns arising from online activity are assessed promptly and referred to children's social care, the police or other relevant agencies where appropriate.
- Ensuring that the school responds appropriately to online abuse, grooming, exploitation, cyberbullying, harmful sexual behaviour and exposure to harmful content.
- Ensuring that staff receive appropriate training to recognise online risks, including the additional vulnerabilities some pupils with SEND or other safeguarding needs may experience.
- Working with the headteacher, ICT personnel and relevant service providers to understand the school's filtering and monitoring arrangements, including how alerts are reviewed and concerns escalated.
- Ensuring that filtering and monitoring concerns which may indicate a safeguarding risk are acted upon promptly and that decisions and actions are recorded.
- Maintaining accurate, confidential and secure records of online safety incidents, disclosures, decisions, actions taken and referrals made.
- Monitoring recorded incidents and concerns to identify recurring patterns, emerging risks and areas where additional education, support or changes to school procedures may be required.
- Ensuring that online safety is embedded within the curriculum and that teaching is adapted where appropriate to meet pupils' ages, developmental stages and individual needs.
- Working with the headteacher and relevant staff to review the effectiveness of online safety arrangements throughout the year and following significant incidents.
- Reporting to the governing board, at least termly, on relevant online safety matters, emerging risks, incidents and the effectiveness of the school's safeguarding arrangements, while maintaining appropriate confidentiality.
- Liaising with the SENCO, class teachers, parents and external agencies where necessary to ensure that pupils affected by online safety concerns receive appropriate support.

The ICT technician will be responsible for:

- Providing technical advice and support to help the school implement its online safety policy and associated procedures.
- Maintaining appropriate technical security measures, including firewalls, anti-virus protection, security updates and access controls, in accordance with agreed responsibilities.
- Supporting the implementation, maintenance and review of the school's filtering and monitoring systems.
- Ensuring that filtering and monitoring systems are maintained and that technical issues affecting their effectiveness are investigated promptly.
- Carrying out regular technical checks, in accordance with the school's agreed arrangements, to help ensure that filtering and monitoring systems remain effective and appropriate.
- Reporting any identified weaknesses, failures or concerns relating to filtering, monitoring or network security to the headteacher and DSL without delay.
- Recording significant technical incidents, changes to filtering arrangements and actions taken to resolve identified issues.
- Working with the headteacher and DSL to assess requests for changes to filtering arrangements, ensuring that safeguarding implications are considered before changes are made.
- Supporting the investigation of suspected cyber security incidents, including malware, phishing, unauthorised access and compromised accounts.
- Advising staff on secure use of devices, accounts, passwords, software and school systems.
- Ensuring that technical arrangements support the school's safeguarding requirements and comply with applicable data protection and cyber security requirements.

All staff members will be responsible for:

- Reading, understanding and complying with this policy, the school's Acceptable Use Agreement, Staff Code of Conduct and other relevant safeguarding policies.
- Completing required safeguarding and online safety training and keeping their knowledge of emerging online risks up to date.
- Modelling safe, respectful and responsible use of technology and maintaining appropriate professional boundaries in all online communications.
- Using school systems, accounts, devices and digital resources appropriately and in accordance with school procedures.
- Taking responsibility for the security of devices, accounts and electronic information they use or access, including protecting passwords and personal or sensitive data.
- Supervising pupils appropriately when they use digital devices, the internet or online learning platforms, taking account of their age, developmental stage and individual needs.
- Teaching and reinforcing safe, respectful and responsible online behaviour where relevant to their role and the curriculum.
- Recognising signs that a pupil may be experiencing online abuse, bullying, grooming, exploitation or other harm.
- Reporting online safety and safeguarding concerns promptly to the DSL or deputy DSL in accordance with the school's safeguarding procedures. Staff must not delay reporting while attempting to investigate concerns themselves.
- Reporting concerns about a member of staff's online behaviour to the headteacher, or to the chair of governors where the concern relates to the headteacher, in accordance with the school's procedures for managing allegations and low-level concerns.
- Reporting suspected cyber security incidents, inappropriate access, breaches of filtering arrangements or loss of devices or data promptly through the school's agreed reporting arrangements.

- Ensuring that online resources, applications and digital tools are assessed for suitability before being used with pupils, in line with school procedures.
- Using artificial intelligence tools only in accordance with the school's agreed requirements, ensuring that confidential, personal or sensitive information is not entered into unauthorised systems.
- Respecting copyright, data protection requirements and the privacy and dignity of pupils and colleagues when creating, accessing or sharing digital content.

Pupils will be responsible for:

- Follow the school's age-appropriate Acceptable Use Agreement and instructions for using digital devices, the internet and online learning resources.
- Treat others with kindness and respect when using technology and communicating online.
- Use school devices, accounts and online resources responsibly and only for their intended educational purposes.
- Keep personal information private and avoid sharing passwords or other people's information without permission.
- Tell a trusted adult if they see something online that worries, upsets or frightens them, or if someone behaves inappropriately towards them online.
- Report concerns about online bullying, harmful content, unwanted contact or other unsafe online behaviour, whether it affects them or another person.
- Follow staff instructions and understand that school devices and online activity may be subject to filtering and monitoring for safeguarding purposes.
- Understand that their online actions can affect themselves and others, and that inappropriate use of technology may be addressed in accordance with the school's Behaviour Policy.

The school will teach pupils how to stay safe online in ways that are appropriate to their age, understanding and individual needs. Pupils will be encouraged to seek help without fear of blame when they encounter difficulties online.

The school recognises that some pupils may need additional support to understand online risks and communicate concerns. Appropriate adjustments and support will be provided where necessary.

Managing online safety

Euxton Primrose Hill Primary School recognises that technology is a significant part of children's lives and can present safeguarding risks both within and outside school. Online safety is therefore an integral part of the school's wider safeguarding responsibilities.

The DSL/headteacher has lead responsibility for online safety, supported by the deputy DSLs, relevant staff and ICT support providers. The school will maintain clear procedures for preventing, identifying, reporting and responding to online safety concerns.

Online safety will be promoted throughout school life through:

- **Staff training:** Staff and relevant governors receive appropriate training and updates to help them recognise online risks and understand their responsibilities.
- **Curriculum:** Online safety is taught through the curriculum, including Computing, Relationships Education and Health Education, and reinforced through everyday learning.
- **Safeguarding procedures:** Online safety concerns are managed in accordance with the Child Protection and Safeguarding Policy and other relevant policies.

- **Filtering and monitoring:** Appropriate technical safeguards are maintained and reviewed to help protect pupils from harmful online content and identify potential safeguarding concerns.
- **Communication with parents and carers:** The school shares relevant information and advice to help families support children's online safety at home.
- **Review and improvement:** Online safety incidents, emerging risks and feedback are considered when reviewing the school's provision and identifying further actions.

The school recognises that some pupils, including those with SEND or other vulnerabilities, may require additional teaching, supervision or support to understand and manage online risks. Online safety provision will be adapted where appropriate to meet pupils' individual needs.

All members of the school community are expected to contribute to a culture in which concerns are reported promptly, children feel able to seek help, and online safety is taken seriously.

Handling online safety concerns

All online safety concerns must be taken seriously and responded to promptly. The safety and welfare of the child will remain the school's primary consideration.

Reporting concerns

- Any member of staff who receives a disclosure or identifies a concern relating to online abuse, bullying, grooming, exploitation, harmful content or inappropriate online behaviour must report it promptly to the DSL or deputy DSL in accordance with the Child Protection and Safeguarding Policy.
- Staff must listen carefully to pupils, take their concerns seriously and reassure them that they have done the right thing by speaking up.
- Staff must not promise confidentiality, conduct their own investigation or delay reporting while attempting to establish all the facts.
- Where there is an immediate risk of harm, staff must take appropriate steps to protect the child and seek urgent assistance where necessary.

Recording and responding to concerns

- The DSL or deputy DSLs will ensure that concerns are recorded securely and accurately using the school's established safeguarding recording procedures.
- Staff must record online safety and safeguarding concerns promptly on CPOMS, in accordance with the school's safeguarding procedures. Where a concern requires an immediate response, staff must report it directly to the DSL or deputy DSL without delay; recording the concern must not delay action to protect a child.
- Records will include relevant information about the concern, decisions made, actions taken, support offered and any referrals to external agencies.
- The DSL will assess the concern and determine the appropriate response, including consultation with children's social care, the police or other relevant agencies where necessary.
- The school will consider whether other pupils may be at risk and whether further safeguarding action or preventative measures are required.
- Parents and carers will be informed where appropriate, unless doing so could increase risk to the child or compromise safeguarding enquiries.
- Online safety incidents will be reviewed to identify recurring patterns, emerging risks and any changes needed to school practice.

Concerns involving staff
Concerns about a member of staff's online behaviour or use of technology must be reported in accordance with the school's procedures for managing allegations and low-level concerns. Concerns about the headteacher must be referred to the chair of governors or the appropriate external authority, in line with the school's safeguarding procedures.

Suspected illegal activity
Where online activity may involve a criminal offence, the DSL and headteacher will consider the appropriate response and seek advice from the police or relevant safeguarding agencies. Staff must not download, forward or unnecessarily copy potentially illegal images or material. Any handling of such material must follow current safeguarding guidance and advice from the relevant authorities.

The school will respond proportionately and take account of the age, understanding, vulnerability and circumstances of the pupils involved. Children who have engaged in harmful online behaviour may themselves have experienced abuse or exploitation, and their safeguarding needs must also be considered.

Online bullying

Online bullying (cyberbullying) involves the use of digital technology to threaten, intimidate, humiliate, harass or deliberately upset another person. It may take place through messaging services, online games, social media, email, shared documents, images or other digital platforms. It can occur at any time and may continue beyond the school day.

Online bullying may include, but is not limited to:

- Sending threatening, abusive, intimidating or upsetting messages.
- Sharing embarrassing, humiliating or manipulated photographs, videos or other content without permission.
- Impersonating another person or using someone else's account to cause harm.
- Posting malicious, defamatory or discriminatory comments online.
- Excluding someone deliberately from online groups or activities to cause distress.
- Repeatedly contacting someone online in an unwanted or intimidating way.
- Sharing private information or encouraging others to target an individual.
- Racist, sexist, homophobic, disablist or other discriminatory abuse.
- Bullying or controlling behaviour within online friendships or relationships.

The school recognises that some pupils, including pupils with SEND or other vulnerabilities, may be at increased risk of experiencing online bullying or may require additional support to recognise and report it.

All concerns about online bullying involving pupils will be taken seriously and reported to the DSL or appropriate member of staff. Incidents will be assessed and addressed in accordance with the Child Protection and Safeguarding Policy and Behaviour Policy, as appropriate.

The school will:

- Support pupils who experience online bullying and take reasonable steps to protect them from further harm.
- Investigate concerns proportionately and consider the needs and circumstances of all pupils involved.

- Take appropriate action in response to bullying, including incidents that occur outside school where they affect pupil welfare, school relationships or the safety of the school community.
- Work with parents and carers where appropriate to resolve concerns and support pupils.
- Teach pupils how to communicate respectfully online, report harmful behaviour and seek help from trusted adults.
- Consider whether an incident involves safeguarding concerns, discriminatory abuse, threats, harassment or potentially criminal behaviour requiring referral to external agencies.

Online bullying will not be dismissed as harmless joking or acceptable behaviour. Pupils will be encouraged to report concerns without fear of blame, and appropriate support will be offered to those affected.

Child-on-child sexual abuse and harassment

The school recognises that child-on-child abuse can occur online as well as face to face. All staff must understand that online sexual harassment and harmful sexual behaviour can affect children of any age and must be taken seriously.

Online sexual harassment and harmful sexual behaviour may include:

- Sending unwanted sexual messages, comments or requests.
- Sharing, threatening to share or encouraging others to share sexualised or intimate images of another person.
- Creating or sharing sexualised images, including images generated or manipulated using artificial intelligence.
- Making sexual comments, jokes or threats online.
- Pressuring, coercing or manipulating another child into sharing images or engaging in sexualised online behaviour.
- Using digital technology to threaten, humiliate, intimidate or control another child.
- Taking or sharing images beneath someone's clothing without their consent, commonly known as upskirting.

All staff must report concerns about online child-on-child sexual abuse or harassment to the DSL or deputy DSL without delay. Concerns will be managed in accordance with the Child Protection and Safeguarding Policy and current statutory guidance.

The school will:

- Take all reports seriously and respond promptly, recognising that children may find it difficult to disclose what has happened.
- Consider the safety and welfare of all children involved, including the child who has experienced harm and any child alleged to have caused harm.
- Assess the risk of further harm, intimidation, retaliation or continued sharing of harmful material.
- Make referrals to children's social care, the police or other relevant agencies where appropriate.
- Work with parents and carers where appropriate and safe to do so.
- Provide age-appropriate education about consent, personal boundaries, respectful relationships, privacy and seeking help.
- Ensure that children are not blamed for abuse or pressured into sharing further details or images.

Sharing nudes and semi-nudes

If a concern involves the creation, possession or sharing of nude or semi-nude images of a child, staff must report it to the DSL or deputy DSL immediately and follow the school's safeguarding procedures and current guidance on responding to such incidents.

Staff must not deliberately view, download, copy, print, forward or share the images. They must not ask a child to send or show them an image. The DSL will determine the appropriate response, including whether advice or a referral to the police or children's social care is required.

The school recognises that a child who has shared an image may have been pressured, groomed, manipulated or exploited. The response will prioritise safeguarding, support and preventing further harm.

Grooming and exploitation

Online grooming occurs when a person builds a relationship or develops trust with a child with the intention of manipulating, exploiting or abusing them. Grooming may be carried out by adults or other children and can take place through social media, online games, messaging services or other digital platforms.

Staff must be aware that children may not recognise that they are being groomed or may feel unable to disclose what is happening because of fear, shame, threats, emotional attachment or manipulation.

Possible indicators of online grooming or exploitation include:

- Becoming secretive about online activity or communications.
- Receiving unexplained gifts, money or new possessions.
- Being contacted by unfamiliar people or individuals whose identity or age is unclear.
- Appearing frightened, distressed or anxious following online interactions.
- Being pressured to keep communications secret, share personal information or send images.
- Being threatened, blackmailed or encouraged to engage in harmful or illegal activity.

These indicators do not necessarily mean that grooming is taking place, but any concerns must be taken seriously.

Child sexual exploitation (CSE) may involve the use of online communication to manipulate, coerce or pressure a child into sexual activity or the production or sharing of sexual images.

Child criminal exploitation (CCE) may involve children being groomed or manipulated online into committing offences or participating in criminal activity for another person's benefit.

The school will:

- Ensure that staff understand the indicators of grooming and exploitation and know how to report concerns.
- Teach pupils, in an age-appropriate way, about safe online relationships, personal boundaries, privacy and seeking help.
- Encourage pupils to tell a trusted adult if someone online makes them feel uncomfortable, asks them to keep secrets or pressures them to do something they do not want to do.
- Report concerns promptly to the DSL or deputy DSL.

- Refer concerns to children's social care, the police or other relevant agencies where appropriate.
- Work with parents and carers where appropriate and safe to do so.
- Provide support to children who may have experienced grooming or exploitation, recognising that they may need reassurance and ongoing safeguarding support.

All concerns will be managed in accordance with the Child Protection and Safeguarding Policy. Staff must not attempt to investigate suspected grooming or exploitation independently.

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

The school recognises that children may be exposed to extremist ideologies, terrorist material and content promoting violence through websites, social media, online games and other digital platforms.

Online radicalisation may involve the manipulation or grooming of children by individuals or groups seeking to influence their beliefs, encourage extremist views or involve them in terrorist-related activity.

Staff will remain alert to concerns that a pupil may be accessing extremist content, being contacted by individuals promoting extremist views or showing signs of being influenced towards violence or terrorism. Online activity alone will not automatically indicate radicalisation; concerns will be considered in context.

The school will:

- Teach pupils, in an age-appropriate way, to think critically about online information, recognise manipulation and seek help when they encounter concerning content.
- Ensure staff understand the indicators of radicalisation and the importance of reporting concerns promptly.
- Report concerns to the DSL or deputy DSL without delay.
- Assess concerns in accordance with the school's safeguarding procedures and Prevent Duty Policy.
- Seek advice or make referrals to relevant safeguarding agencies where appropriate.
- Provide support to pupils who may be vulnerable to radicalisation, taking account of their individual circumstances and safeguarding needs.

All concerns will be handled sensitively and proportionately, with the welfare of the child remaining central to the school's response.

Mental health

The school recognises that online activity can have a significant impact on pupils' emotional wellbeing and mental health. Digital technology can support learning, communication and relationships, but some online experiences may contribute to anxiety, distress, isolation, low self-esteem or other difficulties.

Staff will remain alert to signs that a pupil's online experiences may be affecting their wellbeing, including changes in behaviour, mood, friendships, attendance or engagement in school.

The school will:

- Promote age-appropriate teaching about healthy online habits, respectful relationships and the importance of balancing online and offline activities.
- Help pupils understand how online interactions, social comparison, harmful content and excessive screen use may affect their wellbeing.
- Encourage pupils to speak to a trusted adult if online activity makes them feel worried, upset, unsafe or pressured.
- Ensure staff report safeguarding concerns relating to online activity to the DSL or deputy DSL without delay.
- Provide appropriate support in line with the school's safeguarding and relevant wellbeing procedures.
- Work with parents and carers and, where appropriate, relevant external agencies to support pupils whose online experiences are affecting their wellbeing.
- Consider whether a pupil may be experiencing bullying, grooming, exploitation, harmful content or other safeguarding concerns underlying their distress.

Staff will respond sensitively to pupils' concerns and will not assume that online activity is the sole cause of a change in a child's wellbeing. Where there are concerns about a pupil's safety or mental health, these will be managed through the appropriate school procedures.

Online hoaxes and harmful online challenges

An online hoax is false or misleading information circulated online, sometimes to frighten, confuse or distress others.

A harmful online challenge is an online trend or activity that encourages people to participate in behaviour that may cause physical or emotional harm, either directly or through the creation and sharing of content.

The school recognises that online hoaxes and challenges can spread rapidly through social media, messaging services, online games and other digital platforms. Some may be harmless, while others may pose a significant risk to children's safety and wellbeing.

Staff must report any suspected harmful online challenge or hoax affecting pupils to the DSL or deputy DSL without delay.

The DSL, in consultation with the headteacher where appropriate, will assess the nature and extent of the risk and determine a proportionate response. This will include considering:

- Whether the information is credible and can be verified through reliable sources.
- The potential physical, emotional or safeguarding risks to pupils.
- The age, developmental stage and individual vulnerabilities of the pupils concerned.
- Whether the concern affects individual pupils, particular year groups or the wider school community.
- Whether advice should be sought from the local authority, police or other relevant agencies.
- How to respond without unnecessarily drawing pupils' attention to harmful content or causing additional distress.

The school will:

- Provide age-appropriate guidance to help pupils think critically about online information and recognise potentially harmful trends.
- Encourage pupils to avoid participating in unsafe challenges and to report concerning content to a trusted adult.
- Communicate with parents and carers where appropriate to help them understand the concern and support their children.
- Ensure that any school-wide response is proportionate and does not inadvertently increase pupils' exposure to harmful material.
- Record and manage safeguarding concerns in accordance with the Child Protection and Safeguarding Policy.

The school will prioritise pupils' safety and wellbeing when deciding how to respond and will review its approach as further reliable information becomes available.

Cyber-crime

Cyber-crime involves criminal activity carried out using computers, digital devices or the internet. It includes:

- **Cyber-enabled crime:** Offences that can occur offline but are facilitated or made easier by digital technology, such as fraud, scams and certain forms of exploitation.
- **Cyber-dependent crime:** Offences that can only be committed using computers or digital systems, such as creating or distributing malware, unauthorised access to systems and attacks intended to disrupt digital services.

The school recognises that pupils may encounter cyber-crime or, in some circumstances, become involved in it deliberately or inadvertently.

The school will:

- Teach pupils, in an age-appropriate way, about responsible and lawful use of technology, cyber security and protecting personal information.
- Ensure pupils understand the importance of respecting other people's accounts, devices, data and online privacy.
- Help staff and pupils recognise risks such as phishing, malicious software, online fraud and unauthorised access.
- Require staff to report suspected cyber-crime, suspicious communications, compromised accounts or other cyber security incidents through the school's agreed reporting procedures.
- Ensure safeguarding concerns involving pupils are reported to the DSL or deputy DSL without delay.

- Work with ICT support providers to investigate and respond to technical incidents and protect school systems and data.
- Consider seeking advice from the police or other relevant agencies where criminal activity is suspected.

Where a pupil demonstrates an unusual interest or ability in technology that raises concerns about potentially harmful or unlawful activity, the school will consider the circumstances carefully and respond proportionately. Where appropriate, advice may be sought from relevant support services, including the Cyber Choices programme.

All incidents will be managed in accordance with the school's safeguarding, behaviour, data protection and cyber security procedures.

Online safety training for staff, the curriculum and classroom technology

The school recognises that staff training is essential to maintaining effective online safety and safeguarding arrangements.

The DSL, supported by the headteacher, will ensure that all staff receive appropriate online safety training as part of their induction and ongoing safeguarding training.

Training will cover, as appropriate to staff roles and responsibilities:

- The range of online risks children may encounter, including harmful content, online bullying, grooming, exploitation and child-on-child abuse.
- How technology can facilitate abuse and exploitation, both within and outside school.
- Recognising indicators that a child may be experiencing harm through online activity.
- The school's procedures for reporting, recording and escalating online safety concerns.
- Staff responsibilities for the appropriate use of digital devices, online communication and school systems.
- The purpose and operation of the school's filtering and monitoring arrangements, including how to report concerns or suspected weaknesses.
- Emerging online risks, including artificial intelligence, manipulated images and harmful online trends.
- Cyber security awareness, including phishing, password security and the protection of personal and sensitive information.

The school will provide relevant updates when significant changes in technology, online risks, statutory guidance or school procedures make this necessary.

Staff will be expected to apply their training in their daily practice and seek advice from the DSL or appropriate member of staff if they are uncertain how to respond to an online safety concern.

Completion of required training will be monitored in accordance with the school's staff training and safeguarding procedures.

Online safety and the curriculum

Online safety is embedded throughout the curriculum at Euxton Primrose Hill Primary School. Teaching is designed to help pupils develop the knowledge, understanding and behaviours needed to use technology safely, responsibly and confidently.

Pupils will also be taught, in an age-appropriate way, about online gaming and communication, online advertising and commercial pressures, and the risks associated with in-game purchases, scams and sharing personal or financial information.

Online safety is addressed particularly through:

- Computing.
- Relationships Education.
- Health Education.
- PSHE and other relevant curriculum areas.
- Assemblies, class discussions and responses to emerging online safety concerns.

Online safety teaching will be appropriate to pupils' ages, developmental stages and individual needs. It will be revisited regularly so that pupils can develop their understanding as technology and online risks evolve.

Pupils will be taught, as appropriate to their age and understanding:

- How to recognise and respond to online risks.
- How to evaluate online information and recognise misinformation, disinformation and misleading content.
- How websites, games and online platforms may use persuasive techniques to influence behaviour.
- How to protect personal information and understand their digital footprint.
- What constitutes acceptable and unacceptable online behaviour.
- How to recognise online bullying, grooming, exploitation and other harmful interactions.
- The importance of respectful communication, personal boundaries and privacy.
- How to respond if they encounter upsetting, inappropriate or harmful content.
- How and when to report concerns and seek help from a trusted adult.
- How online activity can affect wellbeing, relationships and safety.
- How to use digital technology, including emerging technologies such as artificial intelligence, safely and responsibly.

The DSL will work with relevant staff to support the development of the online safety curriculum. Class teachers will ensure that online resources are appropriate before using them with pupils, and external resources or visitors will be reviewed for suitability.

The school recognises that some pupils, including those with SEND or other vulnerabilities, may require additional teaching, repetition, visual support or personalised approaches to understand online risks and communicate concerns. Relevant staff will work together to ensure that appropriate adjustments and support are provided.

Staff will create a supportive learning environment in which pupils feel able to ask questions and report concerns without fear of blame. Any safeguarding disclosures arising from online safety teaching will be managed in accordance with the Child Protection and Safeguarding Policy.

The online safety curriculum will be reviewed regularly to ensure that it remains relevant to pupils' experiences, emerging technologies and current safeguarding risks.

Use of technology in the classroom

The school uses a range of digital technologies to support teaching, learning and communication. These may include computers, laptops, tablets, interactive displays, email, cameras, educational applications and online learning platforms.

Before using websites, applications, digital tools or online platforms with pupils, staff must ensure that they are appropriate for the pupils' ages, developmental stages and learning needs. Where required, staff must seek approval in accordance with the school's procedures.

Staff will:

- Use approved digital resources and online platforms wherever possible.
- Check that online resources are suitable and relevant before introducing them to pupils.
- Supervise pupils' use of technology appropriately, taking account of their age, understanding and individual needs.
- Ensure that pupils understand the expectations for safe and responsible use of devices and online resources.
- Report inappropriate content, unsafe functionality or concerns about a digital resource to the appropriate member of staff.
- Respect copyright and ensure that digital materials are used lawfully.
- Protect personal and sensitive information when using online platforms and digital tools.
- Ensure that photographs, videos and other digital content involving pupils are captured, stored and shared in accordance with the school's safeguarding and data protection procedures.

The school will use filtering and monitoring arrangements to help protect pupils when accessing online resources through school systems. These measures do not replace the need for appropriate supervision, professional judgement and clear expectations for pupil behaviour.

Where online learning resources or platforms are recommended for use at home, staff will consider their suitability and any relevant safeguarding or data protection implications.

Any concerns arising from pupils' use of technology in the classroom must be reported and managed in accordance with the school's relevant policies and procedures.

Use of smart technology

The school recognises that smart technology, including mobile phones, smartwatches, tablets and other internet-connected devices, can provide benefits but may also present safeguarding risks.

Pupils may encounter risks through personal devices, including online bullying, unwanted contact, exposure to inappropriate content, sharing of personal information and the creation or distribution of images without consent.

The school will:

- Teach pupils about the safe, responsible and age-appropriate use of smart technology.
- Ensure that expectations for personal devices on school premises are communicated clearly to pupils, parents and carers.
- Manage pupils' use of mobile phones, smartwatches and other personal devices in accordance with the school's agreed arrangements and relevant policies.

- Ensure staff use personal and school-owned technology professionally and in accordance with the Staff Code of Conduct and Acceptable Use Agreement.
- Ensure that photographs, recordings and other digital content involving pupils are captured and shared only in accordance with school procedures.
- Respond promptly to concerns involving the misuse of smart technology, including bullying, harassment, inappropriate images, unwanted contact or access to harmful content.
- Provide age-appropriate guidance to pupils about privacy, online communication, personal boundaries and seeking help.
- Review emerging risks associated with new devices, applications, platforms and online trends.

Concerns arising from the use of smart technology will be managed in accordance with the Child Protection and Safeguarding Policy, Behaviour Policy and other relevant school procedures.

The school's expectations for mobile phones and personal devices will be communicated to parents and carers and reviewed when necessary to reflect changes in technology, safeguarding risks and statutory guidance.

Educating parents

Euxton Primrose Hill Primary School recognises that parents and carers play an important role in helping children stay safe online. The school will work in partnership with families to promote safe, responsible and age-appropriate use of digital technology at school and at home.

Parents and carers will be provided with information about online safety risks and practical advice to help them support their children. This may include guidance on:

- Age restrictions and age-appropriate access to websites, applications, games and social media platforms.
- Parental controls and privacy settings on devices and online services.
- Recognising and responding to online bullying, grooming, exploitation and inappropriate contact.
- Managing screen time and promoting healthy online habits.
- Responding to harmful content, online challenges, scams and misinformation.
- Supporting children who are upset or distressed by online experiences.
- Reporting online safety concerns to the school and seeking further support where necessary.

The school will share online safety information through appropriate channels, which may include:

- Newsletters and weekly communications, including Wake Up Wednesday newsletter, where appropriate.
- Parents' evenings and school events.
- The school website and relevant online resources.
- Direct communication with parents and carers where an individual concern requires discussion or support.

Where an online safety concern affects a pupil, the school will work with parents and carers where appropriate and safe to do so, while ensuring that safeguarding and confidentiality requirements are maintained.

Parents and carers are encouraged to speak to the school if they have concerns about their child's online experiences or require advice about keeping their child safe online.

Internet access

Access to the school's internet network and online services will be managed in accordance with the school's safeguarding, data protection and acceptable use arrangements.

Pupils, staff and other users will be required to follow the relevant Acceptable Use Agreement or equivalent expectations before being granted access to school systems, where applicable.

The school will:

- Ensure that pupils are taught how to use the internet safely, responsibly and appropriately for their age and stage of development.
- Provide access to online resources that support learning and school operations, subject to appropriate filtering, monitoring and supervision.
- Ensure that staff understand their responsibilities when accessing the internet for school-related purposes.
- Manage access for visitors and other authorised users in accordance with school procedures.
- Maintain appropriate records of authorised access where required.
- Restrict or withdraw access where necessary in response to misuse, safeguarding concerns or breaches of the relevant agreement.

All users are expected to use the school's internet connection and online services responsibly and to report inappropriate content, suspicious activity or concerns about online safety promptly.

Internet access does not remove the responsibility of staff to supervise pupils appropriately or to follow the school's safeguarding procedures.

Filtering and monitoring online activity

The governing board will ensure that the school has appropriate filtering and monitoring systems in place to help safeguard pupils and staff when using school networks, devices and online services.

The school will follow the Department for Education's current filtering and monitoring standards and relevant statutory safeguarding guidance. Filtering and monitoring arrangements will be proportionate to the school's needs and the risks associated with its use of technology.

Roles and responsibilities

The governing board has overall strategic responsibility for ensuring that appropriate filtering and monitoring arrangements are in place.

The headteacher, DSL and relevant ICT personnel or service providers will work together to ensure that:

- Roles and responsibilities for managing filtering and monitoring are clearly assigned.
- Systems are appropriate for the age, needs and risk profile of pupils and staff.
- Staff understand how to report concerns and how monitoring alerts are escalated.
- Identified weaknesses, failures or safeguarding concerns are addressed promptly.

Reviewing filtering and monitoring

The school's filtering and monitoring provision will be reviewed at least annually, and sooner where necessary, including following a significant safeguarding incident, the introduction of new technology or a change to network arrangements.

The review will consider:

- What the filtering system blocks and allows.
- Whether monitoring arrangements identify potentially harmful activity promptly.
- The needs and vulnerabilities of pupils, including pupils with SEND.
- The use of school-managed devices, including the one-to-one iPads provided to pupils in Key Stage 2.
- The use of artificial intelligence tools and any associated safeguarding risks.
- Whether staff training, curriculum provision or school procedures need to be updated.

The review will involve the Assistant Headteacher, Headteacher/DSL, ICT support and the Safeguarding Governor. Findings and actions will be documented and followed up.

Filtering arrangements
The school will ensure that filtering systems are configured to block illegal, inappropriate and potentially harmful content, including content that could expose pupils to abuse, exploitation, extremist material or other safeguarding risks.

Filtering arrangements will be reviewed to ensure that they remain effective while avoiding unreasonable restrictions on teaching, learning and legitimate educational resources. The school recognises that no filtering system can eliminate every online risk and that filtering must be supported by appropriate supervision, education and safeguarding procedures.

Any requests for changes or exceptions to filtering arrangements must be referred to the headteacher and assessed with the DSL and relevant ICT support before changes are authorised. Changes must be recorded.

Monitoring arrangements
The school will use appropriate monitoring arrangements to identify potentially unsafe or inappropriate activity on school networks and school-managed devices. Monitoring may include technical alerts, reports of internet activity and staff supervision of pupils using devices.

Monitoring arrangements will include:

- Regular review of monitoring reports, at least weekly, to identify incidents requiring action.
- Immediate escalation of high-risk alerts or incidents involving potential safeguarding harm, malicious activity or serious technical concerns.
- Clear procedures for deciding who reviews alerts, who takes action and how outcomes are recorded.
- Prompt referral of safeguarding concerns to the DSL or deputy DSL.
- Appropriate technical investigation and support from ICT personnel where required.

The school will ensure that users are informed about filtering and monitoring arrangements and how their activity may be monitored.

Responding to incidents
Deliberate attempts to bypass filtering, access prohibited material or misuse school systems will be investigated proportionately and managed in accordance with the Behaviour Policy, Staff Code of Conduct, Disciplinary Policy and other relevant procedures.

Where inappropriate content is accessed accidentally, staff or pupils must report the incident promptly and follow instructions from the appropriate member of staff.

If material suspected to be illegal is encountered, it must not be downloaded, copied, forwarded or deliberately accessed further. The incident must be reported immediately to the DSL or headteacher, who will seek appropriate advice and make referrals to the relevant authorities where necessary.

All significant filtering and monitoring incidents, decisions and actions will be recorded in accordance with the school's safeguarding, technical incident and data protection procedures.

Device Use and Online Safety

At Euxton Primrose Hill Primary School, digital devices are used to support teaching, learning and pupils' digital literacy. All use of devices must be safe, purposeful and appropriate to pupils' age and stage of development.

Key Stage 2 – 1:1 iPads

Pupils in Key Stage 2 are provided with individual iPads to support their learning. Pupils are expected to follow the school's Acceptable Use Agreement and instructions from staff. Staff will teach pupils how to use devices responsibly, protect personal information, recognise inappropriate content and report anything that makes them feel uncomfortable or unsafe.

Key Stage 1 – shared devices

Pupils in Key Stage 1 share devices. Staff provide close supervision and ensure that activities, websites and applications are appropriate to pupils' age and learning needs.

Safe and responsible use

All school devices must be used in accordance with the school's filtering and monitoring arrangements, Acceptable Use Agreements and relevant safeguarding and data protection policies. Staff must consider online safety when planning activities and ensure that pupils receive appropriate supervision.

Pupils must not attempt to bypass security or filtering arrangements, access inappropriate material, share passwords or use devices to bully, threaten or upset others. Any concerns, inappropriate content or suspected misuse must be reported promptly to a member of staff and, where appropriate, the Designated Safeguarding Lead (DSL).

Staff must report lost or stolen devices, suspected malware, security breaches or unauthorised access in accordance with the school's cyber-security procedures.

The school will regularly review its arrangements for device use to ensure that they remain effective and support safe, inclusive and purposeful learning.

Network security

Euxton Primrose Hill Primary School will take appropriate measures to protect its network, systems, devices and information from unauthorised access, cyber-attacks, malware and other security threats.

The school's network security arrangements will be managed in conjunction with the school's ICT support provider and Lancashire County Council, where applicable.

The school will ensure that:

- **Antivirus and security software** is installed where appropriate, kept up to date and managed in accordance with the school's ICT arrangements.
- **Firewalls and network protection** are maintained to help prevent unauthorised access and protect school systems.
- **Software and applications** are installed or approved only through authorised procedures. Staff and pupils must not download or install unauthorised software.
- **Passwords and accounts** are protected. Users must keep passwords confidential, must not share login credentials and must report suspected unauthorised access.
- **Devices are secured** when unattended, with users locking screens or logging out as appropriate.
- **Suspicious emails and attachments** are treated with caution. Users must not open unexpected attachments, follow suspicious links or respond to suspected phishing messages.
- **Security incidents** are reported promptly to the appropriate ICT support contact and, where there is a safeguarding concern, to the DSL.
- **Personal and confidential information** is handled securely in accordance with the school's data protection requirements.

Staff must follow the school's Cyber Security Policy and Acceptable Use Agreement. Any suspected data breach, malware infection, compromised account or other cyber-security incident must be reported immediately so that appropriate action can be taken.

The school will review its cyber-security arrangements regularly and following significant incidents or changes to its systems.

Email Communications

Email is an important communication tool within Euxton Primrose Hill Primary School. All users must use email responsibly, professionally and safely.

Staff email use

- Staff must use their approved school email accounts for school-related business. Personal email accounts must not be used for school business or accessed on school devices where prohibited by school procedures.
- Emails must be professional, respectful and appropriate. Staff should check recipients carefully before sending messages, particularly where personal or confidential information is involved.
- Personal, sensitive or confidential information must only be shared with authorised recipients and through approved secure methods.
- Staff must take care when opening attachments or following links, particularly in unexpected or suspicious emails.
- Suspected phishing emails, spam, malicious attachments or other suspicious communications must be reported in accordance with the school's ICT procedures.

Pupil email use

Pupils at Euxton Primrose Hill Primary School are not provided with individual school email accounts. Where pupils encounter email or email-based communication through approved educational platforms or activities, staff must ensure that access is appropriate to pupils' age and developmental stage and is suitably supervised.

Pupils will be taught not to share personal information, respond to inappropriate messages or communicate with unknown people online. They must tell a trusted adult if a message makes them feel worried, uncomfortable or unsafe.

Reporting concerns
Any email containing bullying, threats, inappropriate content, suspected grooming or other safeguarding concerns must be reported promptly to a member of staff and, where appropriate, the DSL. Suspected cyber-security incidents must also be reported to the school's ICT support provider.

The school will ensure that email use is consistent with its safeguarding, acceptable use, data protection and cyber-security procedures.

Generative artificial intelligence (AI)

Generative artificial intelligence (AI) tools can create text, images, audio, video and other content. They may offer opportunities to support teaching, learning and school administration, but their use must be carefully considered and managed to protect pupils, staff and the school.

Staff use of AI
Staff may use school-approved AI tools for appropriate educational and administrative purposes, where this is consistent with school procedures. Staff must:

- Check the accuracy, reliability and suitability of AI-generated information before using or sharing it.
- Never enter pupils' personal data, safeguarding information, confidential staff information or other sensitive school information into an AI tool unless its use has been explicitly approved through the school's data protection and ICT procedures.
- Ensure that AI-generated resources are age-appropriate, inclusive and free from harmful, discriminatory or misleading content.
- Retain professional responsibility for decisions, communications, teaching materials and other work supported by AI.
- Consider copyright, intellectual property and the potential for AI-generated content to reproduce bias or misinformation.

Pupil use of AI
Pupils may only access or use AI tools where this has been approved by the school and appropriate safeguards are in place. Any use must be suitable for pupils' age and developmental stage, comply with the tool's age restrictions, and be appropriately supervised.

Pupils will be taught, in an age-appropriate way, that AI-generated content may be inaccurate, misleading or biased. They will also learn about protecting personal information, recognising manipulated images and content, and seeking help if AI is used to upset, deceive, threaten or exploit someone.

Pupils must not use AI tools to create or alter images, videos or other content to humiliate, bully, impersonate, threaten or sexually exploit another person. Any suspected misuse must be reported promptly to a member of staff and, where appropriate, the DSL.

Safeguarding, privacy and review

The school will consider the safeguarding, data protection, cyber-security and filtering and monitoring implications before introducing or approving AI tools. The school will review approved uses as technology and guidance develop.

AI must not replace appropriate professional judgement, direct supervision or established safeguarding procedures. Any concern involving AI-generated harmful content, impersonation,

manipulated images or suspected child sexual abuse material must be managed in accordance with the school's safeguarding procedures.

Social Networking and Social Media

Social networking and social media can create safeguarding, privacy and reputational risks for pupils, staff and Euxton Primrose Hill Primary School. All staff must maintain appropriate professional boundaries online and comply with the school's safeguarding, confidentiality and acceptable use requirements.

Staff use of social media

- Staff must use social media responsibly and consider how their online activity may affect their professional role and the school.
- Staff must not use personal social media accounts to communicate privately with pupils or former pupils where this would be inappropriate or contrary to safeguarding guidance.
- Staff must not accept or initiate inappropriate online friendships or interactions with pupils.
- Staff must not share identifiable information, photographs or videos of pupils, families or colleagues without appropriate authorisation and in accordance with school procedures.
- Confidential school information, safeguarding matters and information about individual pupils or staff must never be discussed on personal social media.
- Staff must ensure that their online conduct does not undermine professional boundaries or bring the school into disrepute.

School social media accounts

Only authorised members of staff may publish content on behalf of the school. Posts must be appropriate, accurate and consistent with the school's values, safeguarding arrangements and image-consent procedures. Any concerns about inappropriate comments, messages or content on school-managed accounts must be reported promptly to the headteacher or a designated member of staff.

Pupils and online social networking

Pupils will receive age-appropriate education about social media, including age restrictions, privacy settings, digital footprints, respectful communication and the risks of sharing personal information or images. Staff must not encourage pupils to access platforms that are unsuitable for their age.

Any online bullying, harassment, inappropriate contact, threats, sharing of harmful content or other safeguarding concern must be reported to the DSL and managed in accordance with the school's safeguarding and behaviour procedures.

Parents and carers

Parents and carers will be encouraged to communicate with the school through its approved channels and to raise concerns directly with the school rather than sharing identifiable information about pupils, families or staff on social media.

The school will respond to relevant online safeguarding concerns in accordance with its policies and applicable guidance.

The school website

The school website is an important communication tool for sharing information with parents, carers, prospective families and the wider community. All content published on the Euxton Primrose Hill

Primary School website must be accurate, appropriate and consistent with the school's safeguarding, data protection and online safety requirements.

The headteacher, is responsible for overseeing website content. Staff who contribute information must ensure that it is suitable for publication and follow the school's procedures.

Use of Personal Devices and Mobile Phones

The use of personal mobile phones and other personal electronic devices must not compromise the safeguarding, privacy or welfare of pupils or staff at Euxton Primrose Hill Primary School.

Staff use of personal devices

Staff must follow the school's procedures for personal mobile phones and electronic devices. Personal devices must not be used to photograph, film or record pupils, or to store or share pupil information.

Staff must use school-approved equipment and systems for taking photographs, recording learning or communicating information about pupils. Personal devices must not be used to access, store or transmit confidential school information unless this has been explicitly authorised under the school's procedures.

Staff must maintain professional boundaries when using personal devices and must not exchange personal contact details or communicate privately with pupils through personal accounts or devices.

Any loss of a device containing school information, suspected data breach, inappropriate recording or other safeguarding concern must be reported immediately to the headteacher and/or DSL, as appropriate.

Pupil use of personal devices

Pupils must follow the school's rules regarding mobile phones, smartwatches and other personal electronic devices. Any permitted use must be authorised by the school and must not disrupt learning or compromise the safety, privacy or wellbeing of others.

Pupils must not use personal devices to take photographs, make recordings, share inappropriate content, bully others or access unsuitable material on school premises. Any misuse will be addressed in accordance with the school's behaviour, safeguarding and acceptable use procedures.

Visitors and parents

Visitors and parents must respect the privacy of pupils and staff. They must not photograph, film or record pupils on school premises unless this has been specifically authorised by the school.

The school will ensure that its arrangements for personal devices are communicated clearly and applied consistently.

Monitoring and review

The school recognises that online safety risks and technologies change continually. The effectiveness of this policy and the school's online safety arrangements will therefore be reviewed regularly.

The school will ensure that:

- The headteacher, DSL and ICT support provider undertake termly light-touch reviews of this policy and its implementation.
- The governing board, headteacher and DSL review the policy in full at least annually and following significant online safety incidents or relevant changes to statutory guidance.
- The DSL monitors online safety incidents and concerns to identify patterns, emerging risks and gaps in provision, using this information to inform improvements to practice.
- The DSL reports to the governing board on online safety matters at least termly.
- The effectiveness of filtering and monitoring arrangements is reviewed at least annually, with concerns addressed promptly.
- Staff receive updates and training as appropriate, and changes to this policy are communicated to the school community.

Reporting and recording concerns

All online safety concerns must be reported in accordance with the school's safeguarding procedures. The DSL will ensure that concerns, decisions, actions taken and referrals made are recorded securely and accurately.

Concerns about staff online behaviour must be reported to the headteacher, or to the chair of governors where the concern relates to the headteacher. Suspected cyber-security incidents and technical issues must also be reported to the appropriate ICT support contact.

Attendance and safeguarding

Euxton Primrose Hill Primary School recognises that attendance and safeguarding are closely linked. Changes in a pupil's attendance, including unexplained absences, persistent absence or changes in patterns of attendance, may sometimes form part of a wider safeguarding concern.

Where appropriate, attendance information will be considered alongside other relevant information about a pupil's welfare, including any known online safety concerns.

Staff must remain alert to indications that a pupil may be experiencing online bullying, abuse, exploitation or other harm that could affect their wellbeing or attendance. Any concerns must be reported promptly to the DSL and managed in accordance with the school's Child Protection and Safeguarding Policy and Attendance Policy.

The DSL and relevant staff will work together, where necessary, to ensure that concerns are considered holistically and that appropriate support and referrals are made.

The school will follow current statutory guidance on safeguarding and school attendance and will record and respond to concerns in accordance with its established procedures.

Online harms and risks – curriculum coverage

Subject area	Description and teaching content	Curriculum area the harm or risk is covered in
How to navigate the internet and manage information		
Age restrictions	**Online harm or risk:** Accessing online services, games, applications or content that are not appropriate for a child's age. **Teaching content:** • Understand that some online activities and platforms have age restrictions because their content or features may not be appropriate for younger children. • Understand why age restrictions exist and why they should be followed. • Recognise that some platforms use age verification and understand its purpose. • Understand the age of digital consent and why it matters when using online services. • Know that age-restricted content may be harmful or unsuitable for children.	This risk or harm will be covered in the following curriculum areas: • Health education • Computing
How content can be used and shared	**Online harm or risk:** Pupils may not understand how information, comments, images and other content shared online can be stored, copied, shared with others or used in ways they did not intend. **Teaching content:** • Understand what a digital footprint is and how it develops. • Recognise that online posts, comments, photographs and videos can remain accessible and affect their future. • Understand how cookies collect information about online activity. • Understand that content shared online can be copied, saved, altered or shared beyond its intended audience. • Recognise the importance of thinking carefully before posting or sharing information. • Understand that deleting content does not guarantee that all copies have been removed.	This risk or harm will be covered in the following curriculum areas: • Relationships education • Computing

	• Know how to seek help if personal information or content has been shared inappropriately.	
Misinformation, disinformation and online hoaxes	**Online harm or risk:** Pupils may encounter false, misleading or deliberately deceptive information online, including fake news, conspiracy theories, rumours and online hoaxes. **Teaching content:** • Understand the difference between misinformation (false information shared without necessarily intending to mislead) and disinformation (false information deliberately shared to deceive). • Recognise that not everything published online is accurate or trustworthy. • Learn how to check information against reliable sources. • Recognise that images, videos, headlines and online posts can be edited, taken out of context or designed to mislead. • Understand that online hoaxes and viral challenges may encourage unsafe behaviour. • Know not to share information immediately if they are unsure whether it is true. • Know how to report concerning content and seek help from a trusted adult	This risk or harm will be covered in the following curriculum areas: • Relationships and health education • Computing
Fake websites, scams, fraud and phishing	**Online harm or risk:** Pupils may be deceived by fake websites, fraudulent messages, phishing attempts or online scams designed to obtain personal information, passwords or money. **Teaching content:** • Recognise that some websites, emails, messages and adverts are designed to deceive users. • Understand that phishing messages may encourage users to click links, open attachments or provide personal information. • Identify warning signs, including suspicious links, unexpected requests for information and offers that appear too good to be true.	This risk or harm will be covered in the following curriculum areas: • Relationships education • Computing

	• Understand the importance of protecting passwords and personal information. • Know not to click suspicious links, download unexpected attachments or respond to requests for sensitive information. • Know how to report suspicious online activity and seek help from a trusted adult.	
Personal data	**Online harm or risk:** Pupils may share personal information online without understanding the risks to their privacy, safety or wellbeing. **Teaching content:** • Understand what personal information is, including names, addresses, telephone numbers, passwords, photographs and location information. • Recognise why personal information should be kept private and shared only when appropriate. • Understand that information shared online may be collected, stored or used by other people and organisations. • Learn how privacy settings can help control who sees information. • Understand the importance of using strong passwords and keeping login details confidential. • Know not to share personal information with unknown people online. • Know how to seek help if personal information has been requested, shared or used inappropriately.	This risk or harm will be covered in the following curriculum areas: • Relationships education • Computing
Persuasive design and targeted content	**Online harm or risk:** Online platforms may use features designed to attract and maintain users' attention or show content based on their interests and activity. **Teaching content:** • Understand that some online services are designed to encourage users to spend more time online.	This risk or harm will be covered in the following curriculum areas: • Health education • Computing

	• Recognise features such as autoplay, notifications, likes, rewards and endless scrolling. • Understand that online content and adverts may be selected according to a user's interests or previous activity. • Recognise that repeated exposure to particular content may influence feelings, opinions and behaviour. • Learn to make informed choices about screen time and when to take breaks. • Know how to adjust settings or seek adult support if online content or platform features cause concern.	
Privacy settings	**Online harm or risk:** Pupils may unintentionally expose personal information or content to people they do not know because they do not understand or use privacy settings appropriately. **Teaching content:** • Understand what privacy settings are and how they can help protect personal information. • Know that privacy settings can control who sees posts, photographs, profile information and other content. • Understand that settings may differ between apps, games and online platforms. • Recognise the importance of checking privacy settings and seeking help from a trusted adult when needed. • Understand that privacy settings cannot guarantee complete safety and that information can still be copied or shared. • Know how to report or seek help if someone accesses or shares their information inappropriately.	This risk or harm will be covered in the following curriculum areas: • Relationships education • Computing
Online abuse	**Online harm or risk:** Pupils may experience or witness abusive, threatening, discriminatory or harmful behaviour through online communication, games, social media or other digital platforms.	This risk or harm will be covered in the following curriculum areas:

	Teaching content: • Recognise different forms of online abuse, including threatening messages, harassment, discriminatory language and unwanted contact. • Understand that online abuse can cause distress and that behaviour online can have real-world consequences. • Understand the importance of treating others respectfully when communicating online. • Know how to block or report abusive users where appropriate. • Know not to retaliate or forward harmful content. • Understand how to preserve relevant information safely and seek help from a trusted adult. • Know that concerns involving abuse, exploitation or threats must be reported to a member of staff.	• Relationships education • Computing
Radicalisation	**Online harm or risk:** Pupils may encounter online content, individuals or groups that promote extremist views, encourage hatred or attempt to influence them towards radicalisation. **Teaching content:** • Understand that some online content promotes extreme views, hatred or intolerance. • Recognise that individuals or groups may use online platforms to influence others or encourage harmful beliefs and actions. • Develop critical thinking skills when encountering persuasive or extremist content online. • Understand the importance of respecting different beliefs and identities and recognising discriminatory or hateful behaviour. • Know how to report concerning content or contact from someone promoting extremist views. • Understand that they can speak to a trusted adult if something online makes them feel worried, confused or pressured.	All areas of the curriculum

Online challenges and hoaxes	**Online harm or risk:** Pupils may encounter online challenges, hoaxes or viral trends that encourage dangerous, harmful or inappropriate behaviour. **Teaching content:** • Understand that online challenges and trends can sometimes encourage unsafe behaviour. • Recognise that videos, posts or messages may exaggerate risks, mislead viewers or encourage people to copy dangerous actions. • Understand that online popularity, peer pressure or the desire to gain attention must not take priority over personal safety. • Know not to participate in or share challenges that could harm themselves or others. • Recognise the importance of telling a trusted adult about a concerning challenge or hoax. • Know that harmful content should be reported through appropriate channels and not circulated further.	This risk or harm will be covered in the following curriculum areas: • Relationships education
Violent Content	**Online harm or risk:** Pupils may encounter violent, graphic or disturbing images, videos, games or other online content that is unsuitable for their age and may cause distress or encourage harmful behaviour. **Teaching content:** • Understand that some online content depicts violence or other disturbing behaviour and may be unsuitable for children. • Recognise that violent content can appear unexpectedly through videos, games, messages, websites or social media. • Understand that repeatedly viewing disturbing content may affect feelings and wellbeing. • Know not to search for, share or forward violent or disturbing material. • Know how to close or leave the content and tell a trusted adult if they encounter something upsetting. • Understand how to report inappropriate content and why concerns should be taken seriously.	This risk or harm will be covered in the following curriculum areas: • Relationships education

Fake profiles	**Online harm or risk:** Pupils may encounter fake or misleading online profiles used to deceive, manipulate, bully or exploit others. **Teaching content:** • Understand that people online may not be who they claim to be. • Recognise that profile photographs, names and personal details can be false or misleading. • Understand that accepting requests or communicating with unknown people online can create risks. • Know not to share personal information, photographs or location details with people they do not know and trust. • Recognise warning signs, such as someone asking for secrecy, personal information or inappropriate images. • Know how to block and report suspicious accounts and tell a trusted adult if contact causes concern.	This risk or harm will be covered in the following curriculum areas: • Relationships education • Computing
Grooming	**Online harm or risk:** A person may use online communication to build a child's trust, manipulate them or exploit them. Grooming may involve deception, secrecy, pressure or requests for personal information or images. **Teaching content:** • Understand that grooming can happen online and that perpetrators may pretend to be someone else. • Recognise that someone may gradually build trust before asking for secrecy, personal information, photographs or other inappropriate things. • Understand that gifts, compliments or promises do not mean that someone is safe to trust. • Recognise warning signs, including pressure to keep conversations secret, move to another platform or meet in person. • Know that a child is never to blame for being groomed or manipulated.	This risk or harm will be covered in the following curriculum areas: • Relationships education

	• Know how to stop contact, block or report an account where appropriate, and tell a trusted adult. • Understand that concerns about grooming must be taken seriously and reported promptly to the DSL.	
Unsafe communication	**Online harm or risk:** Pupils may receive inappropriate, manipulative, threatening or unwanted messages through online games, messaging services, websites or other digital platforms. **Teaching content:** • Recognise that not all online communication is safe, respectful or appropriate. • Identify warning signs such as requests for personal information, secrecy, inappropriate images or moving conversations to another platform. • Understand that they do not have to respond to messages that make them feel uncomfortable. • Know not to share personal details, passwords, photographs or location information with unknown people. • Understand how to block and report unwanted contact using available platform features. • Know how to tell a trusted adult if they receive a worrying, threatening or inappropriate message. • Understand that concerns involving possible abuse, exploitation or threats must be reported promptly to the DSL.	This risk or harm will be covered in the following curriculum areas: • Relationships education • Computing
Wellbeing	**Online harm or risk:** Online experiences, including harmful content, cyberbullying, social pressure and excessive use of digital devices, may negatively affect pupils' emotional wellbeing and mental health. **Teaching content:** • Understand that online experiences can affect feelings, confidence, relationships and wellbeing. • Recognise when online activity or interactions are causing worry, distress or pressure.	This risk or harm will be covered in the following curriculum areas: • Health education

	• Understand the importance of balancing screen time with sleep, physical activity, friendships and other interests. • Know that comparing themselves with others online may affect how they feel about themselves. • Understand that they can take a break from online activity and seek help when needed. • Know how to speak to a trusted adult if online experiences affect their wellbeing. • Understand that online bullying and harmful content should be reported rather than endured in silence.	
Self-harm, suicide and eating disorders	**Online harm or risk:** Pupils may encounter online content that promotes, encourages or normalises self-harm, suicide or harmful attitudes towards food, body image and weight. **Teaching content:** • Understand that some online content may encourage harmful behaviours or present them as normal or desirable. • Recognise that online images and messages can create unrealistic expectations about appearance and body image. • Understand that content promoting self-harm, suicide or dangerous eating behaviours can be harmful. • Know not to search for, share or encourage others to engage with harmful content. • Understand the importance of telling a trusted adult if they encounter upsetting content or are worried about themselves or someone else. • Know that pupils experiencing distress should be listened to, supported and referred through the school's safeguarding procedures where appropriate.	This risk or harm will be covered in the following curriculum areas: • Health education