Yohden Primary School
Educational Visits Policy
(including use of social media and mobile and smart technology)

Academic year 2026-27

Key Details

Designated Safeguarding Lead (s): Michaela Lowery, Acting Headteacher

Deputy Safeguarding Lead: Gabrielle Marshall, Acting Deputy Headteacher
Deputy Safeguarding Lead: Gemma Metcalf, EYFS Lead

Named Governor with lead responsibility: Zoe Smith
Named Governor with lead responsibility: Nicola Bell

Date written: September 2026
Date agreed and ratified by Governing Body: October 2026
Date of next review: October 2027

This policy will be reviewed at least annually. It will also be revised following any concerns and/or updates to national and local guidance or procedure.

It is recommended that this policy is accessed electronically so that embedded links take the user to the most up to date documentation.

Contents

1. Policy Aims 3
2. Policy Scope 3
3. Monitoring and Review 4
4. Roles and Responsibilities 4
5. Education and Engagement Approaches 6
6. Reducing Online Risks 8
7. Safer Use of Technology 10
8. Social Media 17
9. Use of Mobile and Smart Technology 20
10. Responding to Online Safety Incidents and Concerns 22
11. Procedures for Responding to Specific Online Incidents or Concerns 23
12. Useful Links and Resources 28

1. Policy Aims

- This online safety policy has been written by Yohden Primary School in consultation with staff, pupils, parents and carers, drawing on Durham County Council and national guidance and specialist advice where required.
- It takes account of the Department for Education's Keeping Children Safe in Education 2026, the Early years foundation stage statutory framework, Working Together to Safeguard Children, the DfE's Filtering and monitoring standards for schools and colleges, and Durham Safeguarding Children Partnership procedures.
- The purpose of this online safety policy is to:
  - Safeguard and protect all members of our school community online
  - Identify approaches to educate and raise awareness of online safety throughout the community
  - Enable all staff to work safely and responsibly, to role model positive behaviour online and to manage professional standards and practice when using technology
  - Identify clear procedures to use when responding to online safety concerns.
- Our school identifies that the issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:
  - **Content:** being exposed to illegal, inappropriate or harmful material
  - **Contact:** being subjected to harmful online interaction with other users
  - **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm
  - **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. We will report any concerns to the Anti-Phishing Working Group

2. Policy Scope

- Online safety is an essential part of safeguarding and acknowledges its duty to ensure that all learners and staff are protected from potential harm online.
- The internet and associated devices, such as computers, tablets, mobile phones and games consoles, are an important part of everyday life.
- Learners should be empowered to build resilience and to develop strategies to manage and respond to risk online.
- This policy applies to all staff including the governing body, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the setting (collectively referred to as “staff” in this policy), as well as learners, parents and carers.
- This policy applies to all access to the internet and use of technology, including personal devices, or where learners, staff or other individuals have been provided with setting issued devices for use off-site, such as work laptops, tablets or mobile phones.

Links with other policies and practices

This policy links with several other policies, practices and action plans including:

Anti-bullying policy

- Acceptable Use Policies (AUP) and/or the Code of Conduct/Staff Behaviour policy
- Behaviour policy
- Safeguarding policy
- Confidentiality policy
- Curriculum policies, such as: Computing, Personal Social and Health Education (PSHE), Citizenship and Relationships and Sex Education (RSE)
- Data Protection

- Image Use policy
- Low Level Concerns
- Searching, Screening and Confiscation policy

3. Monitoring and Review

- Technology in this area evolves and changes rapidly. This policy will be reviewed at least annually.
- The policy will also be revised following any national or local policy requirements, any child protection concerns or any changes to the technical infrastructure.
- We will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.
- To ensure they have oversight of online safety, the *headteacher* will be informed of online safety concerns, as appropriate.
- The named governor for safeguarding will report regularly to the governing body on online-safety practice and incidents, including filtering and monitoring. The governing body will receive a recorded annual assurance review covering system effectiveness, identified risks, actions taken and any changes required.
- Any issues identified via monitoring will be incorporated into our action planning.

4. Roles and Responsibilities

- The Designated Safeguarding Lead (DSL), Mrs Michaela Lowery, has lead responsibility for online safety.
- We recognise that all members of the community have important roles and responsibilities to play with regards to online safety.
- Governors will ensure online safety is a running and interrelated theme whilst devising and implementing our whole-school approach to safeguarding. Our safeguarding governor will monitor this.

The school senior leadership team will:

- Ensure that online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements.
- Ensure there are appropriate and up-to-date policies regarding online safety, including the Staff Code of Conduct and the Yohden Staff Acceptable Use Agreement, which staff read and sign as part of induction and subsequent annual policy acknowledgement.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of systems and networks. Leaders will use the DfE's filtering and monitoring standards and Plan technology for your school tool to support review, planning and improvement.
- Ensure that online safety is embedded within a progressive curriculum, which enables all learners to develop an age-appropriate understanding of online safety.
- Support the DSL and any deputies by ensuring they have sufficient time and resources to fulfil their online safety responsibilities.
- Ensure there are robust reporting channels for the community to access regarding online safety concerns, including internal, local and national support.
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology.
- Audit and evaluate online safety practice to identify strengths and areas for improvement.

The Designated Safeguarding Lead (DSL) will:

- Act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate.

- Work alongside deputy DSLs to ensure online safety is recognised as part of the setting's safeguarding responsibilities and that a coordinated approach is implemented.
- Ensure all members of staff receive regular, up-to-date and appropriate online safety training.
- Access regular and appropriate training and support to ensure they understand the unique risks associated with online safety and have the relevant up to date knowledge required to keep learners safe online.
- Access regular and appropriate training and support to ensure they recognise the additional risks that learners with SEN and disabilities (SEND) face online.
- Keep up-to-date with current research, legislation and trends regarding online safety and communicate this with the community, as appropriate.
- Work with staff to coordinate participation in local and national events to promote positive online behaviour, such as Safer Internet Day.
- Ensure that online safety is promoted to parents, carers and the wider community, through a variety of channels and approaches.
- Maintain records of online safety concerns, as well as actions taken, as part of the settings safeguarding recording mechanisms.
- Monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures.
- Report online safety concerns, as appropriate, to the setting's leadership team/DSL/ Governing Body as appropriate.
- Work with the leadership team to review and update online safety policies on a regular basis (at least annually) with stakeholder input.
- Meet regularly with the governor with a lead responsibility for safeguarding and online safety.

It is the responsibility of all members of staff to:

- Contribute to the development of online safety policies.
- Read and adhere to the online safety policy and acceptable use policies.
- Take responsibility for the security of setting systems and the data they use or have access to.
- Model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site.
- Embed online safety education in curriculum delivery, wherever possible.
- Have an awareness of a range of online safety issues and how they may be experienced by the children in their care.
- Identify online safety concerns and take appropriate action by following the settings safeguarding policies and procedures.
- Know when and how to escalate online safety issues, including signposting to appropriate support, internally and externally.
- Take personal responsibility for professional development in this area.
- Know and contribute to the school filtering and monitoring processes.

It is the responsibility of staff managing the technical environment to:

- Provide technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures.
- Implement appropriate security measures as directed by the DSL and leadership team, to ensure that the setting's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised.

- Ensure that our filtering and monitoring procedures are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team.
- Ensure that our filtering and monitoring systems are applied and updated on a regular basis; responsibility for its implementation is shared with the leadership team
- Ensure appropriate access and technical support is given to the DSL (and/or deputy) to our filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required.

It is the responsibility of learners (at a level that is appropriate to their individual age and ability) to:

- Engage in age-appropriate online safety education opportunities.
- Contribute to the development of online safety policies.
- Read and adhere to the acceptable use policies.
- Respect the feelings and rights of others, both on and offline.
- Take responsibility for keeping themselves and others safe online.
- Seek help from a trusted adult, if there is a concern online, and support others that may be experiencing online safety issues.

It is the responsibility of parents and carers to:

- Read the acceptable use policies and encourage their children to adhere to them.
- Support our online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home.
- Role model safe and appropriate use of technology and social media.
- Abide by the home/school acceptable use policies***.***
- Identify changes in behaviour that could indicate that their child is at risk of harm online.
- Seek help and support from the setting, or other appropriate agencies, if they or their child encounter risk or concerns online.
- Contribute to the development of the online safety policies.
- Use our systems, such as learning platforms, and other network resources, safely and appropriately.
- Take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies.

5. Education and Engagement Approaches

Education and engagement with learners

- The setting will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst learners by:
  - Ensuring education regarding safe and responsible use precedes internet access.
  - Including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSE) and computing programmes of study.
  - Reinforcing online safety messages whenever technology or the internet is in use.
  - Educating learners in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation.
  - Teaching learners to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- The setting will support learners to read and understand the acceptable use policies in a way which suits their age and ability by:
  - Displaying acceptable use posters in relevant areas throughout school.

- Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
- Rewarding positive use of technology.
- Implementing appropriate peer education approaches.
- Providing online safety education and training as part of the transition programme across the key stages and when moving between establishments.
- Seeking learner voice when writing and developing online safety policies and practices, including curriculum development and implementation.
- Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

Vulnerable Learners

- At Yohden Primary School some learners are more vulnerable online due to a range of factors. This may include, but is not limited to, children looked after (CLA) or children with a social worker (CIN), children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- We will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable learners. Online safety education is a key part of our Computing curriculum.
- When implementing an appropriate online safety policy and curriculum, we will seek input from specialist staff as appropriate, including the SENCO, CLA & CIN Designated Teacher.

Training and engagement with staff

We will:

- Provide and discuss the online safety policy and procedures with all members of staff as part of induction.
- Provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates.
  - Through annual safeguarding training, regular safeguarding emails/bulletins and specific training.
  - This will cover the potential risks posed to learners (Content, Contact, Conduct) as well as our professional practice expectations.
- Recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures.
- Make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices.
- Make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation.
- Highlight useful educational resources and tools which staff should use, according to the age and ability of the learners.
- Ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting learners, colleagues or other members of the community.

Awareness and engagement with parents and carers

- At Yohden Primary School we recognise that parents and carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.
- We will build a partnership approach to online safety with parents and carers by:

- Providing information and guidance on online safety in a variety of formats.
    - This will include offering specific online safety awareness training and highlighting online safety at other events such as parent evenings, transition events, fetes and sports days.
- Drawing their attention to the online safety policy and expectations in newsletters, letters, our prospectus and on our website.
- Requesting that they read online safety information as part of joining our community, for example, within our home school agreement.
- Requiring them to read our acceptable use policies and discuss the implications with their children.

6. Reducing Online Risks

Yohden Primary School recognises that technology provides valuable opportunities for learning, communication and creativity. It can also expose pupils to rapidly changing risks, both within and beyond the school environment.

The school uses the four areas of online risk identified in *Keeping Children Safe in Education*: **content, contact, conduct and commerce**. These risks can overlap, and a single incident may involve more than one area.

6.1 Content

Content risks arise when a pupil is exposed to illegal, inappropriate, misleading or harmful material online. This may include:

- Pornographic or sexual content.
- Child sexual abuse material.
- Content promoting violence, self-harm, suicide, eating disorders or dangerous challenges.
- Racist, misogynistic, homophobic, transphobic, extremist or other hateful content.
- Harmful gender stereotypes and material that normalises abusive or controlling behaviour.
- Influencers who promote hate, violence, discrimination, criminality, unrealistic body images or other unhealthy behaviours.
- Misinformation and disinformation, including false news, manipulated evidence and conspiracy theories.
- Deepfakes and other digitally created or altered images, audio and videos.
- AI-generated content that is inaccurate, biased, inappropriate or presented as though it is genuine.
- Generative AI tools and chatbots that provide harmful, misleading or age-inappropriate responses.
- Algorithm-driven content that repeatedly recommends increasingly extreme, harmful or upsetting material.
- Content designed to encourage radicalisation or support terrorism.
- Content promoting gambling, scams, illegal products or inappropriate financial schemes.

The school will teach pupils that online content is not always reliable or truthful. Pupils will learn, at an age-appropriate level, how to question sources, distinguish fact from opinion, recognise manipulation and seek help when they encounter worrying material.

6.2 Contact

Contact risks arise when a pupil interacts with another person or an automated system online in a way that may place them at risk. This may include:

- Contact from unknown adults or other children.
- Grooming for sexual abuse, criminal exploitation, radicalisation or other harmful purposes.

- Grooming through online games, social-media platforms, messaging services, livestreams and group chats.
- Pressure to move conversations onto private or encrypted platforms.
- Requests for personal information, passwords, photographs, videos or live location.
- Sexualised communication or requests for nude or semi-nude images.
- Online coercion, threats, blackmail or extortion.
- Financial sextortion, where a person threatens to share sexual imagery unless money or further images are provided.
- Adults or children pretending to be someone else.
- Harmful interaction through chatbots or AI-generated characters that simulate relationships or encourage inappropriate disclosure.
- Contact through group chats, disappearing messages, gaming chat, livestreaming or anonymous messaging services.
- Harassment, stalking, intimidation or repeated unwanted communication.
- Pressure to participate in harmful challenges, criminal activity or unsafe meetings.

Pupils will be taught not to share personal or confidential information, to be cautious about online identities and to report any communication that makes them feel uncomfortable, frightened, pressured or confused.

6.3 Conduct

Conduct risks arise from the way a pupil or another person behaves online. This may include:

- Cyberbullying, harassment, humiliation or deliberately excluding others.
- Creating, requesting, sharing or forwarding nude or semi-nude images.
- Creating or sharing deepfakes, altered images or false information about another person.
- Using AI or nudification tools to create sexualised or humiliating images of another person.
- Sharing photographs, recordings or personal information without permission.
- Posting offensive, discriminatory, threatening or abusive comments.
- Livestreaming without understanding who can view, record or redistribute the content.
- Unsafe participation in group chats or use of disappearing-message services.
- Revealing personal information, locations, routines or passwords.
- Impersonating another person or accessing another person’s account.
- Plagiarism, cheating or presenting AI-generated work as a pupil’s own.
- Deliberately attempting to access inappropriate or restricted content.
- Using VPNs, proxy services, personal hotspots or other methods to bypass the school’s filtering and monitoring arrangements.
- Taking part in online challenges, hoaxes or activities that could cause physical or emotional harm.
- Creating a digital footprint that may affect the pupil or others in the future.

The school will teach pupils about respectful online behaviour, consent, privacy, copyright, ownership, digital footprints and the consequences of creating or sharing harmful content. Online behaviour affecting the safety or wellbeing of the school community will be addressed regardless of whether it occurred on school premises or using school equipment.

6.4 Commerce

Commerce risks arise when pupils encounter financial activity, advertising or commercial practices online. This may include:

- Phishing, identity theft and other online scams.

- Fraudulent competitions, giveaways and prize offers.
- In-game purchases and pressure to spend money.
- Loot boxes, gambling-style features and gambling content.
- Subscription traps and hidden costs.
- Counterfeit or illegal products.
- Influencer marketing, undisclosed advertising and persuasive content.
- Requests for bank details, payment information, passwords or security codes.
- Online marketplaces and transactions with unknown individuals.
- Financial extortion, including threats linked to sexual imagery.
- Apps, websites or games that collect or sell personal information.
- Misleading claims promoted through AI-generated content or fake endorsements.

Pupils will be taught that online services are often designed to influence their choices and encourage them to spend money, share information or continue using a platform. They will be encouraged to seek permission from a trusted adult before making purchases, providing information or responding to financial requests.

6.5 The school's approach

To reduce these risks, the school will:

- Provide a progressive and age-appropriate online-safety curriculum through computing, PSHE and Relationships and Sex Education.
- Teach pupils about reliable information, respectful relationships, harmful stereotypes, online influence and positive role models.
- Help pupils understand how algorithms, advertising, influencers and AI-generated content can shape what they see and believe.
- Provide additional and appropriately adapted teaching for pupils with SEND or other identified vulnerabilities.
- Maintain appropriate filtering and monitoring systems.
- Ensure that pupils' use of internet-connected technology is appropriately supervised.
- Use only school-approved applications, platforms and AI tools.
- Provide regular online-safety information and training for staff.
- Share relevant advice and support with parents and carers.
- Encourage pupils to report concerns to a trusted adult without fear of blame.
- Respond to online concerns in accordance with the Safeguarding and Child Protection Policy, Behaviour Policy and other relevant school procedures.
- Review online-safety provision in response to incidents, emerging technology, pupil needs and changes to national or local guidance.

No filtering system can remove every online risk. The school will therefore combine appropriate technology, effective supervision, education and clear reporting arrangements to help pupils develop the knowledge, confidence and resilience needed to stay safer online.

7. Safer Use of Technology

Classroom Use

- Our school uses a wide range of technology. This includes access to:
  - Computers, laptops and other digital devices
  - Internet which may include search engines and educational websites
  - Games consoles and other games-based technologies

  - Digital cameras, web cams and video cameras.
- All setting owned devices will be used in accordance with our acceptable use policies and with appropriate safety and security measures in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- We will ensure that the use of internet-derived materials, by staff and learners, complies with copyright law and acknowledge the source of information.
- Supervision of learners will be appropriate to their age and ability.
  - **Early Years Foundation Stage and Key Stage 1**
    - Access to the internet will be by adult demonstration, with occasional directly supervised access to specific and approved online materials, which supports the learning outcomes planned for the learners' age and ability.
  - **Key Stage 2**
    - Learners will use age-appropriate search engines and online tools.
    - Learners will be directed by the teacher to online materials and resources which support the learning outcomes planned for the learners' age and ability.

Artificial Intelligence and Emerging Technology

- The school recognises that generative artificial intelligence can provide educational benefits but may also create safeguarding, privacy, accuracy, copyright and academic-integrity risks.
- Staff must only use AI tools approved by the school and must follow the school's data-protection and acceptable-use requirements. Personal, confidential or special-category information about pupils, families or staff must not be entered into publicly available AI systems.
- AI-generated material must be checked by a member of staff for accuracy, bias, appropriateness and suitability before it is used with pupils or published.
- Pupils may only access approved AI tools as part of planned, age-appropriate learning supervised by a member of staff. Pupils will be taught that AI-generated content may be inaccurate, biased, misleading or fabricated.
- The school will address risks including AI-generated misinformation, impersonation, deepfakes, harmful content and the creation or alteration of sexualised images. Safeguarding concerns involving AI will be reported immediately to the DSL.

Managing Internet Access

- All staff, learners and governors will read and sign the acceptable-use agreement appropriate to their role before being given access to school computer systems, IT resources or the internet. Staff will sign the Yohden Staff Acceptable Use Agreement.

Decision making

- Governors and leaders have ensured that our setting has age and ability appropriate filtering and monitoring in place, to limit learners' exposure to online risks.
- The governors and leaders are aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding.
- Our decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.
- Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from the leadership team; all changes to the filtering policy are logged and recorded.
- The leadership team will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.

- All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard learners; effective classroom management and regular education about safe and responsible use is essential.

Filtering and Monitoring

Yohden Primary School recognises that filtering and monitoring are essential parts of its wider safeguarding arrangements. Filtering helps prevent access to illegal, inappropriate and harmful content, while monitoring helps the school identify concerning activity so that appropriate action can be taken.

The Governing Body has overall strategic responsibility for ensuring that appropriate filtering and monitoring arrangements are in place. The Acting Headteacher and DSL, supported by ICTSS and the responsible governor, oversees these arrangements.

i. Filtering

- Education broadband connectivity is provided through Durham County Council.
- The school uses Smoothwall to filter internet access and restrict access to illegal, inappropriate and potentially harmful content. This includes, but is not limited to, pornography, child sexual abuse material, unlawful terrorist content, racial hatred, extremism, serious violence, self-harm, harmful sexual content, gambling and inappropriate gaming content.
- The school's filtering arrangements use the blocklists provided by the Internet Watch Foundation and Counter Terrorism Internet Referral Unit.
- Filtering applies to all users accessing the school network, including pupils, staff, visitors and guests. It also applies to all school-managed devices, including devices used away from the school premises where technically possible.
- Different levels of access may be provided for pupils, staff and administrators according to their roles and safeguarding needs. Filtering will not unreasonably restrict teaching, learning or school administration.
- Staff must not attempt to bypass the filtering system or use unauthorised VPNs, proxy services, personal hotspots or other methods to access restricted content.
- Where access to restricted content is required for a legitimate educational or professional purpose, a temporary exception may be requested. Any exception must be approved by the Acting Headteacher or another designated senior leader, considered from a safeguarding perspective by the DSL and documented. ICTSS will make any authorised technical changes.
- The school works with ICTSS to ensure that filtering remains active, appropriately configured and suitable for the age, ability and needs of pupils, including pupils with SEND.
- Filtering arrangements will be checked and formally reviewed at least annually by the senior leadership team, DSL, ICTSS and responsible governor. Additional reviews will take place following a safeguarding incident, significant system change or introduction of new technology, including generative AI tools.
- The school will keep a record of filtering checks, identified concerns and resulting actions.

Filtering systems cannot guarantee complete protection. Effective staff supervision and age-appropriate online-safety education therefore remain essential whenever pupils use internet-connected technology.

Responding to unsuitable or harmful content

If a pupil encounters unsuitable or harmful content, they should:

- Stop interacting with the content.
- Avoid clicking, sharing, copying, saving or deleting it.
- Minimise or close the screen where this can be done safely.
- Report it immediately to the supervising member of staff.

The member of staff must:

- Reassure the pupil and avoid blaming them.

- Avoid investigating or viewing the material unnecessarily.
- Record the website address or other relevant details only where this can be done safely and without accessing, copying or sharing illegal content.
- Report the concern promptly to the DSL or a deputy DSL.
- Report any apparent failure of the filtering system to ICTSS.
- Record safeguarding concerns on CPOMS in accordance with the Safeguarding and Child Protection Policy.

The DSL will decide what further action is required, including whether parents or carers should be informed and whether a referral should be made to the police, First Contact, CEOP, the Internet Watch Foundation or another appropriate agency. Parents will not automatically be contacted where doing so could place a child at additional risk or compromise an investigation.

Suspected illegal content must not be copied, downloaded, printed, shared, forwarded or deleted. The device should be secured, and advice sought from the DSL and police where appropriate.

ii. Monitoring

- The school monitors the use of its internet services, network and school-managed devices through a combination of technical monitoring and direct staff supervision.
- Smoothwall monitoring reports and alerts are made available to the Acting Headteacher and DSL, Mrs Michaela Lowery. When she is unavailable, Miss Gabrielle Marshall, Acting Deputy Headteacher and Deputy DSL, will review or coordinate the review of alerts. ICTSS provides technical support and assists the school in reviewing alerts, system performance and identified risks.
- Monitoring applies to school-managed devices used on and, where technically possible, off the school premises.
- Monitoring reports highlighting incidents or concerning activity will be reviewed at least weekly by an appropriately trained member of staff.
- High-risk safeguarding or security alerts will be reported immediately to the DSL or a deputy DSL so that prompt action can be taken.
- Staff supervising pupils using technology must actively monitor how devices are being used. Technical systems do not replace effective classroom supervision.
- All staff must report concerns if:
  - unsuitable or harmful material can be accessed;
  - the filtering or monitoring system appears not to be working;
  - a pupil attempts to bypass filtering;
  - concerning searches, communications or online activity are observed;
  - filtering unreasonably prevents legitimate teaching or administrative activity; or
  - new applications, devices or technologies introduce additional risks.
- Safeguarding concerns identified through monitoring will be managed by the DSL in accordance with the Safeguarding and Child Protection Policy. Incidents, decisions, actions and outcomes will be recorded on CPOMS.
- Technical faults or concerns about the operation of Smoothwall will be reported to ICTSS.
- Monitoring arrangements will take account of the school's pupils and context, including age, SEND, known safeguarding vulnerabilities, curriculum requirements, use of devices away from school and emerging risks such as generative AI and dynamically generated content.
- The school will ensure that monitoring information is only accessed by authorised individuals and is retained and processed in accordance with data-protection, human-rights and privacy legislation.
- Pupils, staff, parents, carers and visitors will be informed that the school operates filtering and monitoring systems when its network and school-managed devices are used.

Managing Personal Data Online

- Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations and Data Protection legislation.
  - Full information can be found in our Data Protection policy.

Security and Management of Information Systems

- We take appropriate steps to ensure the security of our information systems, including:
  - Virus protection being updated regularly.
  - Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems.
  - Not using portable media without specific permission; portable media will be checked by an anti-virus /malware scan before use.
  - Not downloading unapproved software to work devices or opening unfamiliar email attachments.
  - Regularly checking files held on our network,
  - The appropriate use of user logins and passwords to access our network.
    - Specific user logins and passwords will be enforced for pupils in Year 1 and above.
  - All users are expected to log off or lock their screens/devices if systems are unattended.
  - Further information about technical environment safety and security can be found in our Acceptable Use Policy.

Passwords, Accounts and Cybersecurity

Yohden Primary School recognises that secure accounts, devices and systems are essential for protecting pupils, staff and the school's information. All users must follow the school's Acceptable Use Policy, Data Protection Policy and any instructions issued by the school or ICTSS.

Passwords and account security

All users must:

- Use a unique, strong password or passphrase for their school account.
- Avoid using easily guessed information, such as names, birthdays, school names or common words.
- Use a different password for each school system wherever possible.
- Keep passwords and personal identification numbers private.
- Never share passwords with pupils, colleagues, family members or other individuals.
- Never use another person's account or allow another person to use their account.
- Avoid writing passwords down or storing them in an insecure location.
- Use an approved password manager where this has been authorised by the school.
- Use multi-factor authentication wherever it is available, particularly for email, cloud storage, safeguarding, financial and administrative systems.
- Report any unexpected multi-factor authentication request immediately.
- Change a password promptly where compromise is known or suspected, or when instructed to do so following a security incident.
- Report forgotten passwords through the approved school or ICTSS process rather than asking another person to share access.

The school will not require users to change passwords routinely unless there is a safeguarding, technical or security reason. Passwords must be changed immediately if an account may have been compromised.

Staff must not use shared accounts unless the account has been specifically authorised for a defined operational purpose. Wherever possible, systems should allow activity to be linked to an individual user.

Pupil passwords will be managed in a manner appropriate to pupils' age and ability. Staff supporting pupils with passwords must handle this information securely and must not disclose it unnecessarily.

Securing devices

Users must:

- Lock their screen whenever they leave a device unattended.
- Log out of systems when they have finished using them.
- Store school devices securely when they are not in use.
- Ensure that devices are protected by an approved password, passcode or PIN.
- Prevent pupils or unauthorised individuals from accessing staff accounts or confidential information.
- Avoid leaving devices, paperwork or removable storage containing personal information unattended.
- Report lost, stolen or damaged devices immediately to the Headteacher and ICTSS.
- Only connect authorised devices and storage media to the school's systems or network.
- Not disable antivirus software, firewalls, filtering, monitoring or other security controls.
- Not attempt to gain administrator access or alter security settings without authorisation.

School-managed devices used away from the premises remain subject to the school's security, filtering, monitoring and acceptable-use requirements.

Software, applications and updates

Only applications, software, websites, browser extensions, cloud-storage services and artificial-intelligence tools approved by the school may be used for school business or with pupils. Approved core platforms include school-managed email, ClassDojo, CPOMS and Arbor, together with school-managed cloud storage. The school will maintain and periodically review an internal list of approved platforms, storage services and AI tools; anything not listed must be checked and approved before use.

Users must not:

- Download or install unauthorised software, applications or browser extensions.
- Store school information in personal email accounts, personal cloud-storage accounts or unauthorised applications.
- Transfer school information to personal devices unless this has been expressly authorised.
- Bypass security warnings or delay required security updates without an authorised reason.
- Use unsupported or out-of-date devices for accessing confidential school information.

Operating-system, software, browser, antivirus and security updates must be installed promptly. School devices should be configured to receive automatic updates wherever possible. ICTSS will provide technical support and assurance that systems remain appropriately maintained and secure.

New software, online services and applications must be risk-assessed before use. This should include consideration of safeguarding, data protection, age restrictions, security, filtering, monitoring and the provider's use of personal information. A Data Protection Impact Assessment will be completed where required.

Email, phishing and suspicious activity

All users should remain alert to phishing, scams, malicious links and fraudulent requests. Warning signs may include:

- Unexpected requests for passwords, payments or personal information.
- Messages creating urgency, fear or pressure.
- Unfamiliar or slightly altered email addresses.
- Unexpected attachments, links, QR codes or shared documents.
- Requests to bypass normal financial or security procedures.
- Unexpected multi-factor authentication notifications.

- Offers, prizes or refunds that appear too good to be true.
- Messages claiming that an account will be closed unless immediate action is taken.

Users must not click suspicious links, open unexpected attachments, scan unknown QR codes or provide passwords or security codes in response to an unsolicited request.

Suspicious messages or activity must be reported immediately through the school's agreed reporting process and to ICTSS. Where possible, the original message should be retained for investigation without forwarding it to other staff.

Responding to a suspected compromise

Users must immediately report:

- A lost or stolen device.
- A password or account that may have been compromised.
- Unexpected account activity.
- Accidental disclosure of personal or confidential information.
- Malware, ransomware or unusual device behaviour.
- Suspicious login notifications.
- An unexpected multi-factor authentication request.
- Access to systems or information beyond their normal permissions.
- Any attempt to bypass the school's security controls.

The user should stop using the affected account or device where advised, but must not delete files, wipe the device or attempt their own investigation.

The Headteacher, DSL, Data Protection Officer and ICTSS will be informed as appropriate. The school will take action in accordance with its safeguarding, data-protection, business-continuity and incident-response procedures. Relevant external agencies, affected individuals and the Information Commissioner's Office will be notified where legally required.

Any cybersecurity incident that creates a safeguarding concern must also be reported immediately to the DSL and recorded in accordance with the Safeguarding and Child Protection Policy.

Managing the Safety of our Website

- We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).
- We will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.
- Staff or learners' personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.
- The administrator account for our website will be secured with an appropriately strong password.
- We will post appropriate information about safeguarding, including online safety, on our website for members of the community.

Publishing Images and Videos Online

- We will ensure that all images and videos shared online are used in accordance with the associated polices, including (but not limited to) the cameras and image use, data security, acceptable use policies, codes of conduct/behaviour, social media and use of personal devices and mobile phones.

Managing Email

- Access to our email systems will always take place in accordance with data protection legislation and in line with other policies, including confidentiality, acceptable use policies and the code of conduct/behaviour policy.

  - The forwarding of any chain messages/emails is not permitted.
  - Spam or junk mail will be blocked and reported to the email provider.
  - Any electronic communication which contains sensitive or personal information will only be sent using secure and encrypted email.
  - Setting email addresses and other official contact details will not be used for setting up personal social media accounts.
- Members of the community will immediately tell A DSL, Mrs Lowery, Miss Marshall or Mrs Metcalf if they receive offensive communication, and this will be recorded in our safeguarding files/records.
- Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked on site.

Staff email

- The use of personal email addresses by staff for any official setting business is not permitted.
  - All members of staff are provided with an email address to use for all official communication.
- Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, learners and parents.

Learner email

- Learners will sign an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted.
- Whole-class or group email addresses may be used for communication outside of the setting.

Educational use of Webcams

- Our school recognises that use of webcams can be a challenging activity but brings a wide range of learning benefits.
  - All webcam equipment will be switched off when not in use and will not be set to auto-answer.
  - Video conferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.

Users

- Parents/carers will be informed prior to learners taking part in videoconferencing activities.
- Use of webcams will be supervised

Management of Applications (apps) used to Record Children's Progress and Photographs

- We use Tapastry and Class Dojo to track learners progress and share appropriate information with parents and carers.
- Mrs Lowery, Acting Headteacher, is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
- To safeguard learners' data:
  - Only school issued devices will be used for apps that record and store learners' personal details, attainment or photographs.
  - Personal staff mobile phones or devices will NOT be used to access or upload content to any apps which record and store learners' personal details, attainment or images.
  - Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach in the event of loss or theft.
  - All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.

- Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

8. Social Media

Expectations

- The expectations regarding safe and responsible use of social media applies to all members of our school community.
- The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messenger.
- All members of our school community are expected to engage in social media in a positive, safe and responsible manner.
  - All members of our school community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- We will control learner and staff access to social media whilst using setting provided devices and systems on site.
  - The use of social media during setting hours for personal use is permitted.
    - For publishing on school social media channels this is available through the school office or headteacher's log in. For personal use only during official breaks, lunchtime or at the start/end of the school day.
  - Inappropriate or excessive use of social media during setting hours or whilst using setting devices may result in disciplinary or legal action and/or removal of internet facilities.
- Concerns regarding the online conduct of any member of our school community on social media, should be reported to the DSL and will be managed in accordance with our anti-bullying, allegations against staff, behaviour and child protection policies.

Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.
- Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our code of conduct/behaviour policy as part of acceptable use policy.

Reputation

- All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the setting.
  - Civil, legal or disciplinary action may be taken if staff are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.
- All members of staff are advised to safeguard themselves and their privacy when using social media sites. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include (but is not limited to):
  - Setting the privacy levels of their personal sites.
  - Being aware of location sharing services.
  - Opting out of public listings on social networking sites.
  - Logging out of accounts after use.
  - Keeping passwords safe and confidential.
  - Ensuring staff do not represent their personal views as that of the setting.

- Members of staff are encouraged not to identify themselves as employees of our school on their personal social networking accounts; this is to prevent information on these sites from being linked with the setting, and to safeguard the privacy of staff members.
- All members of staff are encouraged to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance our policies and the wider professional and legal framework.
- Information and content that staff members have access to as part of their employment, including photos and personal information about learners and their family members or colleagues will not be shared or discussed on social media sites.
- Members of staff will notify the Leadership Team immediately if they consider that any content shared on social media sites conflicts with their role.

Communicating with learners and parents and carers

- All members of staff are advised not to communicate with or add as 'friends' any current or past learners or their family members via any personal social media sites, applications or profiles.
  - Any pre-existing relationships or exceptions that may compromise this, will be discussed with DSL (or deputy).
  - If ongoing contact with learners is required once they have left the setting, members of staff will be expected to use existing alumni networks or use official setting provided communication tools.
- Staff will not use personal social media accounts to contact learners or parents, nor should any contact be accepted, except in circumstance whereby prior approval has been given by the headteacher.
- Any communication from learners and parents received on personal social media accounts will be reported to the DSL (or deputy).

Learners' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to learners as part of an embedded and progressive education approach, via age-appropriate sites and resources.
- We are aware that many popular social media sites state that they are not for children under the age of 13, therefore, we will not create accounts specifically for learners under this age.
- Any concerns regarding learners' use of social media will be dealt with in accordance with existing policies, including anti-bullying and behaviour.
  - Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.
- Learners will be advised:
  - To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location.
  - To only approve and invite known friends on social media sites and to deny access to others by making profiles private.
  - Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present.
  - To use safe passwords.
  - To use social media sites which are appropriate for their age and abilities.
  - How to block and report unwanted communications.
  - How to report concerns both within the setting and externally.

Official Use of Social Media

- The school's official social media channels are:
  - Facebook

- The official use of social media sites only takes place with clear educational or community engagement objectives, with specific intended outcomes.
  - The official use of social media as a communication tool has been formally risk assessed and approved by the headteacher.
  - Leadership staff have access to account information and login details for our social media channels, in case of emergency, such as staff absence.
- Official social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only.
  - Staff use setting provided email addresses to register for and manage any official social media channels.
  - Official social media sites are suitably protected and, where possible, run and/or linked to/from our website.
  - Public communications on behalf of the setting will, where appropriate and possible, be read and agreed by at least one other colleague.
- Official social media use will be conducted in line with existing policies, including: anti-bullying, image/camera use, data protection, confidentiality and child protection.
  - All communication on official social media platforms will be clear, transparent and open to scrutiny.
- Parents/carers and learners will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the community.
  - Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.
  - Any official social media activity involving learners will be moderated.
- Parents and carers will be informed of any official social media use with learners; written parental consent will be obtained, as required.
- We will ensure that any official social media use does not exclude members of the community who are unable or unwilling to use social media channels.

Staff expectations

- Members of staff who follow and/or like our official social media channels will be advised to use dedicated professionals accounts, where possible, to avoid blurring professional boundaries.
- If members of staff are participating in online social media activity as part of their capacity as an employee of the setting, they will:
  - Sign our social media acceptable use policy.
  - Always be professional and aware they are an ambassador for the setting.
  - Disclose their official role and/or position but make it clear that they do not necessarily speak on behalf of the setting.
  - Always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared.
  - Always act within the legal frameworks they would adhere to within the workplace, including: libel, defamation, confidentiality, copyright, data protection and equalities laws.
  - Ensure that they have appropriate consent before sharing images on the official social media channel.
  - Not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so.
  - Not engage with any direct or private messaging with current, or past, learners, parents and carers.

- Inform their line manager, the DSL (or deputy) of any concerns, such as criticism, inappropriate content or contact from learners.

9. Use of Mobile and Smart Technology

- Our school recognises that personal communication through mobile technologies is an accepted part of everyday life for learners, staff and parents/carers, but technologies need to be used safely and appropriately within the setting.** **

Expectations

- All use of personal devices (including but not limited to; tablets, games consoles and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as anti-bullying, behaviour and child protection.
- Electronic devices of any kind that are brought onto site are the responsibility of the user.
  - All members of our school community are advised to take steps to protect their mobile phones or devices from loss, theft or damage; we accept no responsibility for the loss, theft or damage of such items on our premises.
  - All members of our school community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.
- Mobile phones and personal devices are not permitted to be used in specific areas within the site such as changing rooms, toilets and swimming pools.
- The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the community; any breaches will be dealt with as part of our behaviour policy.
- All members of our school community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our behaviour or child protection policies.
- All members of our school community are reminded that taking covert images typically under clothing (Upskirting) is illegal and will be dealt with as part of the discipline policy.

Staff Use of Mobile and Smart Technology

- Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as relevant policy and procedures, such as: confidentiality, child protection, data security and acceptable use.
- Staff will be advised to:
  - Keep mobile phones and personal devices in a safe and secure place during lesson time.
  - Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times.
  - Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times.
  - Not use personal devices during teaching periods, unless permission has been given by the headteacher, such as in emergency circumstances.
  - Ensure that any content bought onto site via mobile phones and personal devices are compatible with their professional role and expectations.
- Members of staff are NOT permitted to use their own personal phones or devices for contacting learners or parents and carers.
  - Any pre-existing relationships, which could undermine this, will be discussed with the DSL (or deputy)
- Staff will not use personal devices:

  - To take photos or videos of learners and will only use work-provided equipment for this purpose.
  - Directly with learners and will only use work-provided equipment during lessons/educational activities.
- If a member of staff breaches our policy, action will be taken in line with our code of conduct/staff behaviour and allegations policy
  - If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device, or have committed a criminal offence, the police will be contacted.

Learners' Use of Mobile and Smart Technology

- Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- Our school expects learners' personal devices and mobile phones to be…
  - Left at home
  - If they have to be brought to school for safeguarding reasons, they will be handed into the school office at the start of the school day and collected at the end of the day following the signing of the mobile phone contract.
- If a learner needs to contact their parents or carers the school office will contact them on their behalf.
  - Parents are advised to contact their child via the school office
- Mobile phones or personal devices will not be used by learners during lessons or formal educational time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
  - The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.
  - If members of staff have an educational reason to allow learners to use their mobile phones or personal devices as part of an educational activity, it will only take place when approved by the Leadership Team.
- If a learner breaches the policy, the phone or device will be confiscated and will be held in a secure place.
  - Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our behaviour or bullying policy or could contain youth produced sexual imagery (sexting).
  - Searches of mobile phone or personal devices will only be carried out in accordance with our policy.
  - Learners' mobile phones or devices may be searched by a member of the leadership team, with the consent of the learner or a parent/carer. Content may be deleted or requested to be deleted, if it contravenes our policies.
  - Mobile phones and devices that have been confiscated will be released to parents or carers at the end of the day.
  - If there is suspicion that material on a learner's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

Visitors' Use of Mobile and Smart Technology

- Parents/carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with our acceptable use policy and other associated policies, such as: anti-bullying, behaviour, child protection and image use.
- We will ensure appropriate signage and information is displayed and provided to inform parents, carers and visitors of expectations of use.

- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputy) of any breaches our policy.

Officially provided mobile phones and devices

- Members of staff will be issued with a work phone number and email address, where contact with learners or parents/carers is required.
- Setting mobile phones and devices will be suitably protected via a passcode/password/PIN and must only be accessed or used by members of staff.
- Setting mobile phones and devices will always be used in accordance with the acceptable use policy and other relevant policies.

10. Responding to Online Safety Incidents and Concerns

- All members of the community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), cyberbullying and illegal content.
- All members of the community must respect confidentiality and the need to follow the official procedures for reporting concerns.
  - Learners, parents and staff will be informed of our complaints procedure and staff will be made aware of the whistleblowing procedure.
- We require staff, parents, carers and learners to work in partnership to resolve online safety issues.
- After any investigations are completed, we will debrief, identify lessons learnt and implement any policy or curriculum changes as required.
- The school will follow the NSPCC guidance on when to contact the Police available here :-

when-to-call-the-police--guidance-for-schools-and-colleges.pdf (npcc.police.uk)

- If an incident or concern needs to be passed beyond our community (for example, if other local settings are involved or the public may be at risk), the DSL will speak with Durham Police first to ensure that potential investigations are not compromised.

Concerns about Learners' Welfare

- The DSL (or deputy) will be informed of any online safety incidents involving safeguarding or child protection concerns.
- The DSL (or deputy) will record these issues in line with our child protection policy.
- The DSL (or deputy) will ensure that online safety concerns are escalated and reported to relevant agencies in line with the DSCP thresholds and procedures.
- We will inform parents and carers of online safety incidents or concerns involving their child, as and when required.

Staff Misuse

- Any complaint about staff misuse will be referred to the headteacher, in accordance with the safeguarding policy.
- Issues which do not meet the threshold requiring reporting to the LADO will be recorded in the schools record of low level concerns.
- Any allegations regarding a member of staff's online conduct reaching the threshold will be discussed with the LADO (Local Authority Designated Officer).
- Appropriate action will be taken in accordance with our staff behaviour policy/code of conduct.

11. Procedures for Responding to Specific Online Incidents or Concerns

Online Sexual Violence and Sexual Harassment between Children

- Our setting has accessed and understood the guidance and part 5 of Keeping Children Safe in Education 2026
- We recognise that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation.
  - Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our child protection and anti-bullying policy.
- We recognise that internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.
- We also recognise the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.
- We will ensure that all members of the community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSE curriculum.
- We will ensure that all members of the community are aware of sources of support regarding online sexual violence and sexual harassment between children.
- We will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.
- If made aware of online sexual violence and sexual harassment, we will:
  - Immediately notify the DSL (or deputy) and act in accordance with our child protection and anti-bullying policies.
  - If content is contained on learners electronic devices, they will be managed in accordance with the DfE 'searching screening and confiscation' advice.
  - Provide the necessary safeguards and support for all learners involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support.
  - Implement appropriate sanctions in accordance with our behaviour policy.
  - Inform parents and carers, if appropriate, about the incident and how it is being managed.
  - If appropriate, make a referral to partner agencies, such as First Contact and/or the Police.
  - If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community.
    - If a criminal offence has been committed, the DSL (or deputy) will discuss this with Durham Police first to ensure that investigations are not compromised.
  - Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate.

Sharing nudes and semi-nudes

The school's detailed response is set out below in **Sharing Nudes and Semi-Nudes and Suspected Child Sexual Abuse Material**. All concerns must be reported immediately to the DSL or a deputy DSL.

Online Child Sexual Abuse and Exploitation

- We will ensure that all members of the community are aware of online child sexual abuse, including: exploitation and grooming; the consequences; possible approaches which may be employed by offenders to target children and how to respond to concerns.
- We recognise online child sexual abuse and exploitation (including criminal exploitation) as a safeguarding issue and, as such, all concerns will be reported to and dealt with by the DSL (or deputy).
- Schools are reminded that a criminal offence has been committed if a person aged 18 or over intentionally communicates with a child under 16, who the adult does not reasonably believe to be 16 or over, if the communication is sexual or if it is intended to encourage the child to make a communication which is sexual. The offence will be committed whether or not the child communicates with the adult. This is the offence of sexual communication with a child under section 67 of the Serious Crime Act 2015.
- We will implement preventative approaches for online child sexual abuse and exploitation (including criminal exploitation) via a range of age and ability appropriate education for learners, staff and parents/carers.
- We will ensure that all members of the community are aware of the support available regarding online child sexual abuse and exploitation (including criminal exploitation), both locally and nationally.
- We will ensure that the 'Click CEOP' report button is visible and available to learners and other members of our community. If made aware of incident involving online child sexual abuse and we will:
  - Act in accordance with our child protection policies and the relevant Durham SCP procedures.
  - If appropriate, store any devices involved securely.
  - Make a referral to First Contact (if required/appropriate) and immediately inform Durham police via 101, or 999 if a child is at immediate risk.
  - Carry out a risk assessment which considers any vulnerabilities of learner(s) involved (including carrying out relevant checks with other agencies).
  - Inform parents/carers about the incident and how it is being managed.
  - Provide the necessary safeguards and support for learners, such as, offering counselling or pastoral support.
  - Review the handling of any incidents to ensure that best practice is implemented; leadership team will review and update any management procedures, where necessary.
- We will respond to concerns regarding online child sexual abuse and exploitation (including criminal exploitation), regardless of whether the incident took place on our premises or using setting provided or personal equipment.

Where possible, learners will be involved in decision making and if appropriate, will be empowered to report concerns such as via the Click CEOP report: www.ceop.police.uk/safety-centre/.

- If we are unclear whether a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through the Education Durham or Durham Police.
- If learners at other setting are believed to have been targeted, the DSL (or deputy) will seek support from Durham Police and/or Education Durham first to ensure that potential investigations are not compromised.

Sharing Nudes and Semi-Nudes and Suspected Child Sexual Abuse Material

Yohden Primary School recognises that the creation, sharing or possession of nude or semi-nude images involving anyone under the age of 18 is a safeguarding concern. This includes images, videos, livestreams and digitally created or altered content, including AI-generated images and "deepfakes".

The term "sharing nudes and semi-nudes" will be used when referring to images that children or young people have created themselves or shared with other children. "Indecent images of children" is a legal term; however, this policy uses the clearer safeguarding term "child sexual abuse material" where images may have been

created, possessed or distributed by an adult, or where there are concerns about abuse, grooming or exploitation.

All concerns must be reported immediately to the Designated Safeguarding Lead or a deputy DSL. The school will follow its Safeguarding and Child Protection Policy and related safeguarding procedures, current UKCIS and Department for Education guidance, Durham Safeguarding Children Partnership procedures, and advice from the police where appropriate.

Staff must not

Staff dealing with suspected nude or semi-nude imagery or child sexual abuse material must not:

- Intentionally view the image or video unless a decision has been made by the DSL that viewing is unavoidable and necessary to protect a child.
- Copy, print, download or save the content.
- Forward, upload, email or otherwise share the content.
- Photograph, film or screenshot the content.
- Ask a pupil to send, share or display the content.
- Ask a pupil to download or save the content.
- Delete the content or ask a pupil to delete it without advice from the DSL or police.
- Search a device or access its files beyond the school's lawful powers and agreed procedures.
- Describe the content in unnecessary or graphic detail.
- Allow other staff or pupils to view the content.
- Investigate the incident independently or question the pupils involved in detail.

If content appears unexpectedly, the member of staff should stop viewing it as soon as possible, avoid closing or deleting files where this could alter evidence, secure the device and report the matter immediately to the DSL.

Initial staff response

When a concern is reported or discovered, the member of staff should:

- Respond calmly and reassure the pupil that they have done the right thing by reporting the concern.
- Avoid blame, judgement or promises of confidentiality.
- Establish only the basic information needed to safeguard the pupil, without conducting an investigation.
- Avoid viewing the imagery or asking the pupil to show it.
- Record what the pupil has said using their own words.
- Report the concern immediately to the DSL or a deputy DSL.
- Record the safeguarding concern on CPOMS in accordance with the school's Safeguarding and Child Protection Policy.
- Secure any school-owned or confiscated device without examining its files or content.

Any device will be managed in accordance with the DfE's Searching, Screening and Confiscation guidance. A device must not be searched simply to establish whether an image exists. Police advice will be sought where there may be evidence of an offence, abuse, exploitation or significant harm.

DSL response

The DSL or deputy DSL will hold responsibility for coordinating the school's response. They will:

- Consider the immediate safety and welfare of every child involved.
- Consider whether there is a risk of further sharing, coercion, blackmail, exploitation, bullying, humiliation or retaliation.
- Consider the age, understanding, vulnerability and additional needs of the children involved.

- Consider whether the imagery was created or shared consensually, under pressure, through grooming, or without the knowledge of the child depicted.
- Consider whether an adult is involved.
- Consider whether the content has been created, manipulated or altered using artificial intelligence or other digital tools.
- Consider whether any child involved has a social worker, an Education, Health and Care Plan or other identified vulnerabilities.
- Decide whether the incident can be managed internally or requires referral to First Contact, the police, CEOP, the LADO or another agency.
- Make sure that decisions, actions and reasons are recorded clearly on CPOMS.
- Provide appropriate safeguarding, pastoral and educational support to the children involved.
- Review relevant filtering, monitoring, behaviour and curriculum arrangements following the incident.

The DSL will ordinarily avoid viewing the imagery. A decision to view it will only be made in exceptional circumstances where this is unavoidable and necessary to safeguard a child. The reasons for the decision, who viewed it and the outcome must be recorded. Wherever possible, advice should be sought from the police before viewing suspected illegal imagery.

Immediate referral

The DSL will seek immediate advice from the police and/or children's social care where:

- An adult is suspected of creating, possessing, requesting or sharing sexual imagery involving a child.
- There are concerns about grooming, sexual abuse, criminal exploitation or commercial exploitation.
- A child has been pressured, coerced, blackmailed or threatened.
- The imagery depicts sexual acts or is unusually explicit or violent.
- The imagery involves a child who is, or appears to be, under 13.
- A child is at immediate risk of significant harm.
- The content has been shared widely or uploaded publicly.
- There are concerns that the imagery forms part of an organised or repeated pattern.
- The identity or age of those involved cannot be established.
- The school is unable to manage the risk safely without external support.

If there is an immediate danger to a child or a crime is in progress, the school will contact the police on 999.

Concerns involving a member of staff, volunteer, contractor or other adult working with children will be referred immediately to the Headteacher and managed under the school's allegations procedures. The LADO will be contacted where the harm threshold may be met. Concerns involving the Headteacher will be reported to the Chair of Governors.

Informing parents and carers

Parents and carers will normally be informed at an early stage and involved in supporting their child. However, the DSL may delay or withhold notification where informing a parent or carer could:

- Place a child at increased risk of harm.
- Lead to the loss or destruction of evidence.
- Interfere with a police or social-care investigation.
- Place another child at risk.
- Be contrary to advice from children's social care, the police or another safeguarding agency.

The reasons for any decision about parental involvement will be recorded.

Recording and retaining information

Written records should include only the information necessary to explain the concern, assess risk and document the school's response. Staff must not include copies, screenshots or unnecessarily detailed descriptions of sexual imagery within CPOMS, emails, reports or other school records.

The school will not retain copies of suspected nude or semi-nude images or child sexual abuse material. Any device or material required as evidence will only be retained or transferred following police advice and will be stored securely with access strictly restricted.

The school will not delete suspected illegal content unless instructed to do so by the police or another authorised agency.

Removing content and supporting pupils

Where content has been shared online, the DSL will support the child and family to report and remove it safely. This may include support through:

- The platform's reporting and blocking tools.
- Childline and the Internet Watch Foundation's Report Remove service.
- CEOP, where there are concerns about online sexual abuse or exploitation.
- The Internet Watch Foundation, where child sexual abuse material has been published online.
- Police or social-care support where required.

The school will provide proportionate pastoral support and will consider the needs of all children involved, including the child depicted, any child who has shared the content and any child who has received it.

Any disciplinary response will be considered alongside the school's safeguarding duties, the child's age and understanding, the circumstances of the incident and any evidence of coercion, abuse or exploitation. Safeguarding and support will not be replaced by a solely punitive response.

The school will respond to these concerns regardless of whether the incident occurred on school premises, away from school, on a school-managed device or on a personal device, where the incident affects the safety or welfare of pupils or the school community.

Child Criminal Exploitation – Including County Lines

- All staff need to be aware of the indicators that a child may be at risk from, or involved with Child Criminal Exploitation (CCE) and note that this can be facilitated through the use of technology. Further details are in the schools safeguarding policy.

Cyberbullying

- Cyberbullying, along with all other forms of bullying, will not be tolerated at our school.
- Full details of how we will respond to cyberbullying are set out in our anti-bullying policy.

Online Hate

- Online hate content, directed towards or posted by, specific members of the community will not be tolerated at our school and will be responded to in line with existing policies, including anti-bullying and behaviour.
- All members of the community will be advised to report online hate in accordance with relevant policies and procedures.
- The Police will be contacted if a criminal offence is suspected.
- If we are unclear on how to respond, or whether a criminal offence has been committed, the DSL (or deputy) will obtain advice through First Contact or Durham Police

Online Radicalisation and Extremism

- We will take all reasonable precautions to ensure that learners and staff are safe from terrorist and extremist material when accessing the internet on site.

- If we are concerned that a child or parent/carer may be at risk of radicalisation online, the DSL (or deputy) will be informed immediately, and action will be taken in line with our child protection policy.
- If we are concerned that member of staff may be at risk of radicalisation online, the headteacher will be informed immediately, and action will be taken in line with the child protection and allegations policies.

12. Useful Links and Resources

Local safeguarding and support

Durham Safeguarding Children Partnership.

Emergency: call 999 where a child is in immediate danger or a crime is in progress. For non-emergency police enquiries, call 101.

First Contact: use Durham's current local safeguarding referral route and procedures.

ICTSS helpdesk: 03000 261100.

Local Authority Designated Officer (LADO): 03000 268835. Confirm named contacts and extensions against Durham County Council's current directory before publication.

National guidance for schools

Keeping Children Safe in Education.

Filtering and monitoring standards for schools and colleges.

Generative artificial intelligence in education.

Plan technology for your school.

Sharing nudes and semi-nudes: advice for education settings.

Searching, screening and confiscation.

UK Safer Internet Centre: Professionals Online Safety Helpline.

Internet Watch Foundation.

CEOP Safety Centre.

Advice and reporting for pupils and families

Childline.

Report Remove.

Childnet.

Internet Matters.

NSPCC online safety.

Action Fraud.