Oxhill Nursery School

Online Safety Policy
(including use of social media and mobile and smart technology)

September 2025

Key Details

Designated Safeguarding Lead: Julia Watson

DSL Deputy: Clare Donoghue, Cheryl Lindoe, Georgia Young

Named Governor with lead responsibility: Joe Lalgee

Date written: September 2025

Date agreed and ratified by Governing Body: November 2025

Date of next review: September 2026

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

Contents

Oxhill Nursery School Online Safety Policy

1. **Policy Aims**

- This online safety policy has been written by Oxhill Nursery School involving staff, learners and parents/carers, building on the Kent County Council/The Education People/Durham County Council online safety policy template, with specialist advice and input as required.
- It takes into account the DfE statutory guidance Keeping children safe in education 2025, EYFS statutory framework for group and school-based providers 2025, 'Working Together to Safeguard Children' 2023 and the Durham Safeguarding Children Partnership (durham-scp.org.uk) 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 content, for example: pornography, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation (including fake news) and conspiracy theories (KCSIE 2025, Paragraph 135).
  - **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**

- 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 a work laptops, tablets or mobile phones.

a. **Links with other policies and practices**

This policy links with several other policies, practices and action plans including: Acceptable Use Policies (AUP) and/or the Code of Conduct/Staff Behaviour policy

- Behaviour policy
- Safeguarding policy/Child Protection Policy
- Confidentiality policy
- Data Protection
- Image Use policy
- Low Level Concerns

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 on a regular basis to the governing body on online safety practice and incidents, including filtering and monitoring processes.
- Any issues identified via monitoring will be incorporated into our action planning.

4. **Roles and Responsibilities**

- The Designated Safeguarding Lead (DSL), Julia Watson has lead responsibility for online safety. ***Whilst activities of the designated safeguarding lead may be delegated to an appropriately trained deputy, overall the ultimate lead responsibility for safeguarding and child protection, including online safety remains with the DSL*.**
- 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.

a. **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 a staff code of conduct/behaviour policy *and* acceptable use policy, which covers acceptable use of technology.
- Ensure that suitable and appropriate filtering and monitoring systems are in place and work with technical staff to monitor the safety and security of our systems and networks. For further detail see DfE guidance on meeting digital and technology standards in schools and colleges.
- 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.

- Ensure that all appropriate action to meet the Cyber security standards for schools and colleges Meeting digital and technology standards in schools and colleges - Cyber security standards for schools and colleges - Guidance - GOV.UK is taken to improve our resilience against cyber-attacks.

b. **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.

c. **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 setting's 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.

d. **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 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.
- Ensure that the technology & all processes are in line with the Meeting digital and technology standards in schools and colleges - Filtering and monitoring standards for schools and colleges - Guidance - GOV.UK

e. **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.

f. **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 agreement and/or 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 Class Dojo, 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**

a. **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.
  - 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:
  - Informing learners that network and internet use will be monitored for safety and security purposes and in accordance with legislation.
  - Implementing appropriate peer education approaches.
  - Providing online safety education and training
  - Using support, such as external visitors, where appropriate, to complement and support our internal online safety education approaches.

b. **Vulnerable Learners**

- We recognise that some learners are more vulnerable online due to a range of factors. This may include, but is not limited to, children in care (CiC) 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.

c. **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.

- *as part of existing safeguarding and child protection training/updates or within separate or specific online safety sessions.*
- This will cover the potential risks posed to learners (Content, Contact, Conduct and Commerce), 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.

d. **Awareness and engagement with parents and carers**

- 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**

- We recognise that the internet is a constantly changing environment with new apps, devices, websites and material emerging at a rapid pace.
- We will:
  - Regularly review the methods used to identify, assess and minimise online risks.
  - Examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the setting is permitted.
  - Ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material.
  - Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via our computers or devices.
- All members of the community are made aware of our expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which

could cause harm, distress or offence to members of the community. This is clearly outlined in our acceptable use policies and highlighted through a variety of education and training approaches.

7. **Safer Use of Technology**

a. **Classroom Use**

- Our school uses a range of technology. This includes access to:
  - Computers, laptops and other digital devices
  - Internet which may include search engines and educational websites
  - Learning platform/intranet
  - Email
  - 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.**
- The setting will use age-appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our community.
  - ***The Smoothwall filtering system used in most Durham schools ensures that when using Google it is automatically set to safe search. This reduces but does not eliminate the risk of links to inappropriate content.***
- 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**
    - 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.

b. **Managing Internet Access**

- All staff, will read and sign an acceptable use policy before being given access to our computer system, IT resources or internet.

c. **Filtering and Monitoring**

Note: A guide for education settings about establishing 'appropriate levels' of filtering and monitoring can be found at: *https://www.saferinternet.org.uk/advice-centre/teachers-and-school-staff/appropriate-filtering-and-monitoring*

i **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.
- We will ensure that we will refer to relevant filtering & monitoring DFE guidance in the use of AI in school: Generative AI: product safety expectations - GOV.UK.

ii **Filtering**

- Education broadband connectivity is provided through ***Durham County Council***
- We use ***Smoothwall*** which blocks sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature. We are also aware of the filtering detecting other safeguarding issues, such as self-harm, serious violent crime or issues with county lines grooming.
- The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.
- All school devices should be connected to a filtered feed. If a school device needs access to additional content, for instance to manage official social media, the filter settings for that device or user should be modified to allow access to that content.
- We work with ***ICTSS*** to ensure that our filtering policy is continually reviewed.
- If staff discover unsuitable sites, they will be required to:
  - **turn off monitor/screen and report the concern immediately**
  - The member of staff will report the concern (including the URL of the site if possible) to the DSL (or deputy) and/or technical staff.
  - The breach will be recorded and escalated as appropriate.
  - Parents/carers will be informed of filtering breaches involving their child.
- Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the UK Safer Internet Centre, Durham Police or CEOP.

iii **Monitoring**

- We will appropriately monitor internet use on all setting owned or provided internet enabled devices. This is achieved by:
  - *physical monitoring (supervision), monitoring internet and web access (reviewing logfile information)*
  - ***Smoothwall provides reports about usage that could potentially indicate an issue which requires further investigation. Alerting e-mails are sent to The Headteacher who then takes appropriate action.***
- If a concern is identified via monitoring approaches we will:
  - ***DSL or deputy will respond in line with the child protection policy.***
- All users will be informed that use of our systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

- We will use the Plan technology for your school - GOV.UK to assess ourselves against the filtering and monitoring standards and receive personalised recommendations on how to meet them.

d. **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.

e. **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.
  - 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:
    - **The acceptable use policy**

f. **Password policy**

- All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.
- We require all users to:
  - Use strong passwords for access into our system.
  - Change their passwords every at least annually.
  - Always keep their password private; users must not share it with others or leave it where others can find it.
  - Not to login as another user at any time.

g. **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) What maintained schools must or should publish online - GOV.UK.
- 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.

h. **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.

i. **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 the headteacher 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.

i **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 and parents.

j. **Management of live online meetings and lessons**

- Our school recognises that the use of live online meetings / lessons may be used to enhance the learning opportunities of our pupils and can bring a range of learning benefits.
- Staff will ensure that live online meetings / lessons are suitably risk assessed.
- When necessary, we use a combination of live teaching (online lessons) and recorded teaching (e.g. Oak National Academy lessons, video / audio recordings made by teachers) to teach pupils remotely.

Keeping devices secure

- All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:
  - Keeping the device password-protected – strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
  - Ensuring the hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
  - Making sure the device locks if left inactive for a period of time
  - Not sharing the device among family or friends
  - Installing antivirus and anti-spyware software

- Keeping operating systems up to date – always install the latest updates

Users

- Staff will ensure that only staff and pupil school accounts and systems are used to access live online meetings/lessons.
- Only key administrators will be given access to online lesson administration areas.

Content

- When recording a live online lesson, it should be made clear to all parties at the start of the session. The reason for the recording must be given and recorded material will be stored securely. Staff must be aware of any child who does not have consent to be photographed or filmed and should make appropriate adjustments to safeguard.
- If third party materials are included, we will check that recording is permitted to avoid infringing the third-party intellectual property rights.
- We will establish dialogue with external partners before taking part in a live online lesson. If it is a non-educational establishment, staff will check that the material they are delivering is appropriate for the learners.

k. **Management of Applications (apps) used to Record Children's Progress**

- We use Class Dojo to track learners progress and share appropriate information with parents and carers.
- The *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**

a. **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 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 not*** permitted.
    - 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.

b. **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 *headteacher*
- 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).

- **Official Use of Social Media The school's official social media channels are:**
  - ***Facebook*** ***https://www.facebook.com/p/Oxhill-Nursery-School-100063685023061/***
  - ***YouTube channel*** *https://www.youtube.com/@oxhillnurseryschool9506.*
  - ***Instagram*** ***https://www.instagram.com/oxhill_nursery_school?igsh=MW51NThjMnZienh2eQ==***
- 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* linked *to* 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 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* 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) and/or the *headteacher* 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.

a. 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 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 classrooms, changing areas and toilets

- 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.

b. **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 ***written*** permission has been given by the *headteacher* such as in emergency circumstances.
  - Ensure that any content brought 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) *or headteacher*
- 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.

c. **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) or *headteacher* of any breaches our policy.

d. **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 or *headteacher/manager* will speak with Durham Police first to ensure that potential investigations are not compromised.

a. **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.

b. **Staff Misuse**

- Any complaint about staff misuse will be referred to the *headteacher/manager*, in accordance with the safeguarding policy.
- Issues which do not meet the threshold requiring reporting to the LADO will be recorded in the school's 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.

c. **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 to members of our community. Via our ***website.*** 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.

d. **Indecent Images of Children (IIOC)**

- We will ensure that all members of the community are made aware of the possible consequences of accessing Indecent Images of Children (IIOC).
- We will respond to concerns regarding IIOC on our equipment and/or personal equipment, even if access took place off site.
- We will seek to prevent accidental access to IIOC by using an Internet Service Provider (ISP) which subscribes to the Internet Watch Foundation block list and by implementing appropriate filtering, firewalls and anti-spam software.
- If we are unclear if a criminal offence has been committed, the DSL (or deputy) will obtain advice immediately through Durham Police and/or the Education Safeguarding Team.

- If made aware of IIOC, we will:
  - Act in accordance with our child protection policy and the relevant Durham SCP procedures.
  - Store any devices involved securely.
  - Immediately inform appropriate organisations, such as CEOP, Durham Police or the LADO.
- If made aware that a member of staff or a learner has been inadvertently exposed to indecent images of children, we will:
  - Ensure that the DSL (or deputy) is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
  - Ensure that any copies that exist of the image, for example in emails, are deleted.
  - Report concerns, as appropriate to parents and carers.
- If made aware that indecent images of children have been found on the setting provided devices, we will:
  - Ensure that the DSL (or deputy) is informed.
  - Ensure that the URLs (webpage addresses) which contain the suspect images are reported to the Internet Watch Foundation via www.iwf.org.uk .
  - Ensure that any copies that exist of the image, for example, in emails, are deleted.
  - Inform the Police via 101 (999 if there is an immediate risk of harm) and First Contact
  - Only store copies of images (securely, where no one else has access to them and delete all other copies) at the request of the police only.
  - Report concerns, as appropriate to parents and carers.
- If made aware that a member of staff is in possession of indecent images of children on setting provided devices, we will:
  - Ensure that the *headteacher* is informed in line with our managing allegations against staff policy.
  - Inform the Local Authority Designated Officer (LADO) and other relevant organisations in accordance with our managing allegations against staff policy.
  - Quarantine any devices until police advice has been sought.

e. **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.

f. **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.

g. **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

h. **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.

11. The Use of AI (Artificial Intelligence) in School

We ensure that all use of AI in our school is adopted and monitored in line with the following DFE guidance and Keeping children safe in education 2025 :

Generative AI: product safety expectations - GOV.UK

Using AI in education settings: support materials - GOV.UK

12. Useful Links for Educational Settings

Durham Safeguarding Children Partnership (DSCP)
Durham Safeguarding Children Partnership (durham-scp.org.uk)

Durham Police:
In an emergency (a life is in danger or a crime in progress) dial 999. For other non-urgent enquiries contact the Police via 101
NPCC have produced a useful guide about detailing at what point The Police should be contacted.
when-to-call-the-police--guidance-for-schools-and-colleges.pdf (npcc.police.uk)
Prevent Officer – Steven Holden but referrals should be made through First Contact.

Other:

- ICTSS helpdesk 03000 261100

- Sharon Lewis / Louise Brookes (LADO) 03000 268835

National Links and Resources for Educational Settings:

- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Internet Matters: www.internetmatters.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Parent Protect https://www.parentsprotect.co.uk/ - this includes advice for parents on peer-on-peer abuse and how to cope if your child has got into significant trouble online.
- NSPCC: www.nspcc.org.uk/onlinesafety
- ChildLine: www.childline.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk
- Professional Online Safety Helpline: www.saferinternet.org.uk/about/helpline
- 360 Safe Self-Review tool for schools: www.360safe.org.uk
- Parentzone (Google Internet Legends) https://parentzone.org.uk/
- Lucy Faithful Foundation: Home - Shore

National Links and Resources for Parents/Carers:

- Internet Matters: www.internetmatters.org

This site is particularly useful for providing clear information and up-to-date advice on setting parental controls.

- Action Fraud: www.actionfraud.police.uk (This is the place to report ransomware, scams etc.)
- CEOP:
  - www.thinkuknow.co.uk
  - www.ceop.police.uk
- Childnet: www.childnet.com
- Get Safe Online: www.getsafeonline.org
- Internet Watch Foundation (IWF): www.iwf.org.uk
- Parent protect - advice for parents having difficulties e.g. Peer on peer abuse or Police involvement www.parentsprotect.co.uk/
- NSPCC: www.nspcc.org.uk/onlinesafety
- ChildLine: www.childline.org.uk
- Net Aware: www.net-aware.org.uk
- The Marie Collins Foundation: www.mariecollinsfoundation.org.uk
- UK Safer Internet Centre: www.saferinternet.org.uk