

Oyster Bay Nursery

Online Safety Policy

Date written: October 2026

Date of last update: October 2026

Date agreed and ratified by October 2026

Date of next full review: September 2027

This policy will be reviewed at least annually and/or following any lessons learnt and/or updates to national or local guidance and procedures.

Designated Safeguarding Lead (DSL)	Debra Hines
Deputy Designated Safeguarding Lead(s)	Grace Sidders Rachel Finch
Nominated Individual	Debra Hines
Nursery Manager	Grace Sidders

1. Policy Statement

At Oyster Bay Nursery, we recognise that digital technology plays an important role in modern life and can provide opportunities to support children's learning, communication and development. However, we also recognise that internet-connected devices, online platforms and digital communication can expose children, families and staff to risks.

We are committed to protecting children from inappropriate online content, harmful communication, misuse of personal information and other online safeguarding risks. We aim to create a safe environment in which technology is used responsibly, appropriately and only where it supports children's learning, wellbeing or the effective operation of the nursery.

This policy applies to all staff, volunteers, students, agency workers, visitors and other individuals who use digital technology in connection with Oyster Bay Nursery. It also outlines expectations for parents and carers when communicating with the nursery or sharing information about children online.

The policy must be read alongside our Safeguarding and Child Protection Policy and other relevant nursery procedures.

2. Aims

This policy aims to:

- Safeguard children from inappropriate or harmful online content and contact.
- Ensure digital technology is used safely, appropriately and under suitable supervision.
- Promote age-appropriate understanding of online safety.
- Protect children's, families' and staff members' personal information.
- Establish clear expectations for staff use of devices, online platforms and digital communication.
- Reduce the risk of inappropriate images, videos or information being accessed, recorded, stored or shared.
- Ensure online safety concerns are recognised, reported and addressed promptly.
- Work in partnership with parents and carers to promote safe digital habits.

3. Scope

This policy applies to the use of:

- Computers, laptops, tablets and internet-connected devices.

- Mobile phones, cameras and recording equipment.
- Nursery management systems and parent communication applications (Ovivio).
- Email, messaging services and social media.
- Websites, search engines, online videos and digital learning resources.
- Internet-connected toys, smart devices and other digital equipment.
- Artificial intelligence (AI) tools and other emerging technologies, where relevant to nursery activities.
- Personal devices used by staff, volunteers or visitors in connection with nursery activities.

The policy applies on nursery premises, during outings and trips, and whenever individuals are undertaking duties or communicating on behalf of Oyster Bay Nursery.

4. Children's Access to Digital Technology

Children's use of digital technology will be age-appropriate, purposeful, limited to what is suitable for their developmental stage and appropriately supervised.

The nursery recognises that young children learn most effectively through play, relationships, conversation, movement and practical experiences. Digital technology will not replace these important opportunities.

Where digital devices or online resources are used, staff will:

- Select content appropriate to the child's age, understanding and individual needs.
- Use trusted websites, applications and resources approved by the nursery.
- Supervise children closely throughout the activity.
- Ensure children cannot freely access unrestricted internet content.
- Use suitable filtering, parental controls or restricted-access settings where available.
- Check online content and applications before introducing them to children.
- Avoid exposing children to inappropriate advertising, pop-ups, disturbing images or unsuitable videos.
- Ensure digital activities support learning, creativity, communication or other identified developmental aims.

- Respect children's individual needs, including any sensory, communication or accessibility requirements.
- Stop the activity immediately if unsuitable content appears or a safeguarding concern arises.

Children will not be permitted to access social media, online chat rooms, unrestricted video platforms or other services that are unsuitable for their age.

Children will not be required to use digital technology as a condition of participating in nursery activities.

5. Teaching Children About Online Safety

Although many children attending nursery are very young, we recognise the importance of beginning to develop safe and sensible digital habits from an early age.

Staff will support children's understanding through simple, age-appropriate messages and practical guidance, including:

- Using digital devices with a trusted adult.
- Asking an adult for help if something unexpected or upsetting appears on a screen.
- Understanding that not everything seen or heard online is suitable for children.
- Respecting other people's privacy and personal information.
- Not taking or sharing photographs of others without appropriate permission and adult involvement.
- Using devices gently and following staff instructions.

Online safety learning may be incorporated into stories, discussions, role play and everyday activities. Staff will adapt explanations to children's developmental stage and communication needs.

6. Staff Responsibilities and Professional Conduct

All staff and other adults working at Oyster Bay Nursery must use digital technology responsibly and maintain appropriate professional boundaries.

Staff must:

- Follow this policy and all relevant safeguarding procedures.
- Use nursery-approved devices, systems and accounts for work-related activities wherever required.

- Access only appropriate websites, applications and online content while working.
- Ensure children are supervised when digital devices are being used.
- Never use digital technology to shame, threaten, intimidate or otherwise harm a child.
- Never access, download, display or share inappropriate material on nursery equipment or in the presence of children.
- Never use personal social media accounts to communicate privately with children.
- Never share children's personal information, photographs or videos without proper authorisation.
- Report suspected online abuse, inappropriate content, data breaches or misuse of technology promptly.
- Maintain confidentiality when working with children's records and nursery information.

Staff must not use nursery devices or accounts for unlawful, offensive or inappropriate purposes.

Any use of digital technology that could place a child at risk, breach confidentiality or undermine professional boundaries may result in investigation and appropriate disciplinary or safeguarding action.

7. Mobile Phones, Cameras and Recording Devices

Mobile phones, cameras and recording equipment must be used in accordance with the nursery's Mobile Phone and Camera Policy and Children’s Image Use Policy.

Staff, volunteers and visitors must not use personal devices to photograph, film or record children during nursery activities.

Only authorised devices and approved procedures may be used to capture images or recordings for legitimate nursery purposes.

Where photographs or videos are taken, the nursery will ensure that:

- Appropriate permissions and lawful grounds for use have been established.
- Images are captured only for an authorised purpose.
- Images are stored securely and accessed only by authorised individuals.
- Images are shared only through approved channels.

- Images are not stored on personal devices or personal cloud accounts.
- Unnecessary copies are not made or retained.
- Requests to withdraw permission for optional image use are handled appropriately.

Staff must not take photographs or recordings of children for personal use or share them through personal messaging services or social media.

8. Online Communication with Parents and Carers

Oyster Bay Nursery may use approved digital systems, email or other authorised communication channels to communicate with parents and carers and share information about children's experiences, progress and care.

Staff must:

- Use authorised nursery communication systems and accounts (Ovivio).
- Ensure messages are professional, accurate and appropriate.
- Check recipients before sending information.
- Avoid sharing confidential information through unsecured or unauthorised channels.
- Follow nursery procedures when communicating sensitive safeguarding or health information.
- Keep appropriate records of significant communications where necessary.
- Refer complex, sensitive or contentious matters to the Nursery Manager.

Staff must not exchange personal contact details with parents for unauthorised work-related communication or use personal social media or messaging accounts to discuss children.

Parents and carers should use the nursery's agreed communication channels for enquiries, updates and concerns. Urgent safeguarding matters should be reported directly to the Nursery Manager or Designated Safeguarding Lead (DSL), rather than relying solely on an online message.

9. Social Media and Online Reputation

Staff, volunteers and other individuals working at the nursery must follow the nursery's Social Media Policy.

They must not:

- Post photographs, videos or identifiable information about children without proper authorisation.
- Discuss individual children, families, colleagues or confidential nursery matters on social media.
- Publish information that could identify a child's attendance, routines, location or personal circumstances.
- Make unauthorised statements on behalf of Oyster Bay Nursery.
- Post abusive, discriminatory, threatening or confidential material relating to the nursery or its community.
- Use social media to discuss complaints or safeguarding concerns involving individual children.

Staff should consider how publicly available online content and interactions may affect their professional responsibilities and the trust families place in the nursery.

Any official nursery social media accounts must be managed by authorised individuals, with appropriate access controls and oversight.

10. Personal Devices and Remote Access

Personal devices must not be used to access, photograph, download or store children's confidential information unless the Nursery Manager has expressly authorised a specific arrangement and suitable safeguards are in place.

Staff must not:

- Store children's photographs or records on personal devices.
- Use personal email accounts to transfer nursery records.
- Save confidential information to personal cloud storage.
- Allow unauthorised individuals to access nursery systems using their account.
- Share passwords or leave devices unlocked where confidential information may be accessed.

Any authorised remote access to nursery systems must follow the nursery's security arrangements. Staff must protect devices against unauthorised access and ensure confidential information cannot be viewed by others.

11. Passwords, Accounts and Cybersecurity

Oyster Bay Nursery will take reasonable steps to protect its digital systems and information from unauthorised access, loss, damage and misuse.

Staff must:

- Use individual accounts and secure passwords where provided.
- Keep passwords confidential and never share them with unauthorised people.
- Use multi-factor authentication where available and appropriate.
- Lock devices when unattended.
- Install updates and security measures as directed by the nursery.
- Avoid opening suspicious links, attachments or messages.
- Use only approved software, applications and online services for nursery business.
- Report suspected phishing, malware, unauthorised access or lost devices immediately.

Access to nursery systems will be limited to individuals who need it for their role. Access should be amended or withdrawn when a person changes role or leaves the nursery.

12. Artificial Intelligence and Emerging Technology

Staff must not enter children's personal information, identifiable photographs, safeguarding records or confidential nursery information into public AI tools or unapproved online services.

Any proposed use of AI or other emerging technology for nursery activities or administration must be approved by the Nursery Manager and assessed for suitability, privacy, security and safeguarding risks.

AI-generated information must not be treated as a substitute for professional judgement, qualified advice or established safeguarding procedures. Staff remain responsible for checking the accuracy and appropriateness of any information used in their work.

Children must not use AI tools independently. Any age-appropriate activity involving such technology must be specifically approved, directly supervised and suitable for the children involved.

13. Internet-Connected Toys and Devices

Internet-connected toys, smart speakers, cameras and other devices can collect information or record sounds and images.

Before introducing such devices, the nursery will consider:

- Whether the device is necessary and appropriate for the setting.
- What information it collects and where that information is stored.
- Whether microphones, cameras or recording functions can be disabled.
- Who can access the device or its associated account.
- Whether the device meets the nursery's privacy, security and safeguarding requirements.
- Whether an appropriate risk assessment or data protection assessment is required.

Devices that present unacceptable risks to children's privacy or safety will not be used.

14. Online Safety Incidents and Safeguarding Concerns

Any online safety concern must be taken seriously and reported promptly.

Examples include:

- A child accessing inappropriate online content.
- A child being exposed to upsetting, violent or sexual material.
- Suspected online grooming, exploitation, harassment or abuse.
- Unauthorised photographs or recordings of children.
- Inappropriate online communication involving a child or member of staff.
- Suspected hacking, phishing or unauthorised access to nursery systems.
- Personal information or images being shared without authorisation.
- A lost device containing confidential information.

Staff must report child-related concerns immediately to the DSL or Nursery Manager and follow the Safeguarding and Child Protection Policy.

Staff must not investigate suspected abuse themselves, confront a suspected perpetrator in a way that could increase risk, or promise confidentiality. Relevant information should be preserved where safe and appropriate, without downloading, copying or circulating harmful material unnecessarily.

Where a child may be at immediate risk of harm, staff must take immediate protective action and contact the police or emergency services where necessary.

The DSL or Nursery Manager will determine the appropriate response, which may include contacting parents where safe and appropriate, seeking advice from children's

social care, reporting to the police, notifying the relevant regulatory body or following data breach procedures.

A suspected personal data breach must be reported internally without delay so that the nursery can assess whether notification to the Information Commissioner's Office (ICO) or affected individuals is required.

All incidents and actions taken will be recorded securely and reviewed to identify any necessary improvements.

15. Filtering, Monitoring and Risk Assessment

The nursery will consider the online risks associated with its devices, internet connection, applications and digital activities.

Where children have access to internet-enabled devices, suitable safeguards will be used to reduce the risk of inappropriate access. These may include restricted user profiles, content filtering, disabling unnecessary functions and direct adult supervision.

The Nursery Manager will review the suitability of digital resources and consider whether additional safeguards are needed when introducing new technology.

Any filtering or monitoring arrangements will be proportionate to the nursery's setting, the devices in use and the risks identified. Staff must not assume that technical filters remove the need for active supervision.

16. Parents and Carers

Parents and carers play an important role in promoting online safety and protecting children's personal information.

Oyster Bay Nursery encourages parents and carers to:

- Discuss age-appropriate online safety with their children.
- Supervise children's use of digital devices at home.
- Use suitable parental controls and age-appropriate content settings.
- Avoid posting identifiable photographs or personal information about other children.
- Respect other families' privacy during nursery events.
- Follow nursery rules concerning mobile phones, photography and recording.
- Report concerns about online activity involving a child to the Nursery Manager or DSL.

Parents and carers must not photograph or record other children at nursery unless expressly permitted under the nursery's procedures.

The nursery will share relevant online safety information with families where appropriate and may provide guidance on safe digital habits and suitable resources.

17. Training and Staff Awareness

Staff will receive information and guidance appropriate to their role so that they understand online safety risks and their responsibilities.

Training and induction will cover, as appropriate:

- Recognising online safeguarding risks.
- Safe use of digital devices and online resources.
- Confidentiality and data protection.
- Appropriate online communication and professional boundaries.
- Reporting and recording online safety incidents.
- The nursery's mobile phone, camera and social media procedures.

The Nursery Manager will ensure that staff are informed of relevant policy updates and emerging risks.

18. Monitoring and Review

The Nursery Manager will monitor the implementation of this policy and review it regularly, including after significant online safety incidents, changes in technology or relevant changes to legislation and statutory guidance.

Any updates will be communicated to staff and other relevant individuals.

Related Policies

- Safeguarding and Child Protection Policy
- Mobile Phone and Camera Policy
- Children’s Image Use Policy
- Social Media Policy
- Data Protection and Privacy Policy
- Whistleblowing Policy
- Complaints Policy

- Health, Safety and Risk Assessment Policy
- Visitors Policy