**Online Safety Policy & Procedure**

Table of Contents

[**Introduction** 2](#_Toc156564185)

[ Purpose 2](#_Toc156564186)

[ Scope 2](#_Toc156564187)

[ Relevant legislation and guidance 2](#_Toc156564188)

[**Online Safety Policy** 2](#_Toc156564189)

[ Roles and Responsibilities for Nursery Management, 2](#_Toc156564190)

[ Roles and Responsibilities for All Staff, Students and Volunteers 2](#_Toc156564191)

[ Roles and Responsibilities for Parents and Visitors 6](#_Toc156564192)

[ Compliance and Disciplinary Measures 6](#_Toc156564193)

[**Online Safety Processes and Procedures** 7](#_Toc156564194)

[ Reporting a Concern 8](#_Toc156564195)

[ Incident Response Procedure: 9](#_Toc156564196)

[ Policy Changes 10](#_Toc156564197)

[ Key Contacts 10](#_Toc156564198)

[**Policy management and review** 11](#_Toc156564199)

**Introduction**

At The Little Bumblebee Nursery, we prioritize the well-being and safety of our children. In today's digital age, we've established a comprehensive Online Safety Policy addressing all electronic devices, social media, and image sharing. Our commitment is to create a secure environment fostering positive interactions while safeguarding privacy. This policy guides staff and parents in promoting responsible and safe online practices, aligning with our values.

* Purpose

The Little Bumblebee Nursery is dedicated to offering a secure and nurturing early childhood education. Our purpose is to cultivate emotional, social, and intellectual growth through innovative learning experiences. We are committed to educational excellence, embracing diversity, collaborating with parents, and preparing children for life's challenges. Our goal is to guide each child in a journey of discovery, fostering a lifelong love for learning and enabling positive contributions to the world.

* Scope

This policy applies to all individuals affiliated with The Little Bumblebee Nursery, governing the responsible use of electronic devices, social media, and image sharing. It outlines guidelines for staff, parents, and guardians to ensure a secure online environment within and outside the nursery premises. Regular updates will be made to align with evolving technologies and best practices.

* Relevant legislation and guidance
* Data Protection Act (DPA)
* Children's Online Privacy Protection Act (COPPA)
* Education (Care Standards) (Wales) Regulations 2016
* UK Council for Internet Safety (UKCIS) Guidelines
* The Little Bumblebee Nursery's Code of Conduct

**Online Safety Policy**

* Roles and Responsibilities for Nursery Management,
* Recognition of Online Safety as part of Safeguarding: Managers should ensure that online safety is recognized as part of the setting's safeguarding responsibilities, with the Designated Safeguarding Lead (DSL) taking the lead.
* Reporting and Actioning Online Safety Concerns: Managers should ensure that online safety concerns are reported to the DSL, recorded, and actioned.
* Children's Involvement in Online Safety: Managers should ensure that children are enabled to share online concerns at a level appropriate to their age and ability.
* Inclusion of Online Safety in Safeguarding Policy: The Safeguarding policy should include procedures for handling online safety concerns.
* Roles and Responsibilities for All Staff, Students and Volunteers
* Understanding Safeguarding Responsibility: Staff should understand their safeguarding responsibility and how it fits into their role on a day-to-day basis.
* Familiarity with Policies: Staff should be familiar with the setting's policies relevant to online safety, including an Acceptable Use Policy (AUP).
* Communication and Contact Policies: Staff should be aware of policies regarding staff contact outside of work, ensuring professional communication channels and transparency.

1. **Information Communication Technology (ICT):**

* *Access:* Only ICT equipment belonging to the nursery setting is used by both staff and children.
* *Responsibility for Equipment Safety:* The nursery manager is responsible for ensuring that all ICT equipment is safe and fit for its intended purpose.
* *Secure Access and Monitoring:* Managers should ensure that access to the setting's network and IT infrastructure is secure, with appropriate filtering and monitoring in place.
* *Secure Data Management:* Managers should ensure that personal data is managed securely online, following GDPR and data protection requirements.
* *Virus Protection:* All computers used in the nursery have virus protection software installed to safeguard against potential threats.
* *Safety Settings:* The designated person is responsible for configuring safety settings on ICT equipment to prevent access to inappropriate material.
* *Staff Supervision and Safe Technology Use:* Staff should appropriately supervise children using devices, check apps and websites before use, and model safe technology practices.

1. **Internet Access**

*Children's Internet Access:*

* Children do not normally have unsupervised access to the Internet.

*Staff Access to Internet Use for Learning*

* If staff access the Internet for children's learning, written parental permission is obtained after showing parents this policy.
* The designated person has overall responsibility for ensuring children's safeguarding, and risk assessments related to online safety are conducted.

*Teaching Stay Safe Principles:*

* Children are taught age-appropriate stay safe principles before using the Internet, including:
* Going online only with a grown-up present.
* Keeping information about themselves safe.
* Pressing only buttons online that they understand.

*Building Resilience and Addressing Issues:*

* Designated persons work to build children's resilience in the online world, addressing issues like staying safe, fostering appropriate friendships, asking for help when unsure, and not keeping secrets. This is done as part of social and emotional development in age-appropriate ways.

*Second-hand Computers:*

* If a second-hand computer is acquired, the designated person ensures no inappropriate material is stored on it before children use it.

*Computer Placement:*

* All computers for children's use are located in areas clearly visible to staff.

*Reporting Suspicious Material:*

* Staff report any suspicious or offensive material, including content that may incite racism, bullying, or discrimination, to the Internet Watch Foundation at www.iwf.org.uk.

*Reporting Inappropriate Contact:*

* Suspicions of an adult attempting inappropriate contact with a child online are reported to the National Crime Agency's Child Exploitation and Online Protection Centre at www.ceop.police.uk.

*Access to Resources:*

* The designated person ensures staff have access to age-appropriate resources to assist children in using the internet safely.

1. **Email**

* *Children's Email Usage:* Children are not permitted to use email within the setting.

*Parent and Staff Email Access:*

* Parents and staff are generally not permitted to use nursery equipment for accessing personal emails.

*Staff Email Usage with Children:*

* Staff do not access personal or work email while supervising children.
* *Secure Transmission of Personal Information:* Staff ensure that personal information is sent via encrypted email for security.Information sharing is conducted securely at all times.

1. **Mobile phones**

* *Children's Possession:* Ensure that children do not possess their mobile phones or other ICT devices during nursery sessions. If found, these devices are to be removed and stored securely in a locked safe until parents collect them at the session's end.
* *Staff Mobile Phone Usage:* Staff may bring their mobile phones to work, but these must be securely placed in the locked safe located in the office before any contact with children.
* Mobile phones will be kept in a designated secure location and returned to staff members during lunch breaks and at the end of their shifts. It is strictly prohibited for staff to take photographs or videos of children using unauthorized devices. Additionally, personal mobile phones should not be used on the premises while caring for children during working hours.
* To ensure compliance, all personal mobile phones are stored securely in a locked safe in the office. Staff members are required to place their phones into a designated box, which remains locked throughout nursery hours. Phones may only be used during lunch breaks when no children are present. The manager conducts regular checks after each lunch break to ensure that all phones are returned to the box and securely locked away.
* *Emergency Usage:* We recognise that people may wish to have their personal mobile phones at work for use in case of emergency. Personal mobile phones may be used in emergency situations, but only in areas where there are no children present and with prior permission from the manager. The staff should provide family and friends with the nursery mainline in case of emergency.
* *Mobile Phones on Outings:* If staff or volunteers bring their mobile phones on outings for emergency use, they are prohibited from making or receiving personal calls or taking photographs of children.
* *Theft or Damage to Property:* All mobile phone phones are brought into the nursery at the owner’s risk and the nursery will not be held liable for damage or theft of the phones.
* *Contact Information:* Staff and volunteers ensure that the nursery's telephone number is known to family members and others who may need to contact them in case of an emergency.
* *Application of Rules:* These rules also extend to the use of work-issued mobile phones and apply when staff visit or support colleagues in other settings.

**Cameras and videos**

* *Personal Cameras and Recording Equipment:* Staff and volunteers are prohibited from bringing personal cameras or video recording equipment into the nursery setting.
* *Photographs and Recordings:* Photographs and recordings of children are only taken for valid reasons, such as recording their learning and development or for displays within the setting. Written permission from parents, as indicated in the Registration form, is mandatory. The manager monitors such use.
* *Parental Requests and General Permission:* If parents request permission to photograph or record their own children at special events, general permission must be obtained from all parents for their children to be included. Parents are informed that they do not have the right to photograph anyone else's child or upload photos of other children.
* *Publicity Use of Photographs:* If photographs of children are used for publicity purposes, parental consent is required, and safeguarding risks are minimized. For instance, ensuring children cannot be identified by name or by being photographed in a sweatshirt with the name of the nursery on it.

**Social media**

This policy encompasses the use of all forms of social media, including platforms like Facebook, LinkedIn, Twitter, and blogs, applicable for both business and personal use during or outside office hours. The policy extends to the use of social media on our IT facilities, as well as personal equipment owned by staff.

* *Restrictions on Social Networking:* Children are not allowed to access social networking sites.
* *Discretion in Social Media Use:* Staff members are expected to exercise discretion on social media, refraining from sharing information or images related to nursery activities or children in their care.
* *Staff Cooperation:* Staff cooperation is essential in upholding these standards. Disciplinary procedures are outlined in staff handbooks for further details.
* *Personal Security Settings:* Staff are advised to manage personal security settings to control information access, limiting it to people they choose to share information with.
* *Professional Conduct:* Staff should not accept service users, children, and parents as friends on social media, as it breaches expected professional conduct.
* *Organization Mention on social media:* When staff mention the organization or workplace on social media, they do so in a way that is not detrimental to the organization or its service users.
* *Confidentiality and Work-Related Discussions:* Staff observe confidentiality and refrain from discussing work-related issues on social media.
* *Information Sharing Caution:* Staff should not share information they wouldn't want children, parents, or colleagues to view.
* *Reporting Concerns:* Staff are required to report any concerns or breaches to the designated person in their setting.
* *Personal Communication Boundaries:* Staff avoid personal communication, including on social networking sites, with children and parents with whom they act in a professional capacity. If a practitioner and family are friendly prior to the child coming into the setting, this information is shared with the manager before a child attends, and a risk assessment and agreement on boundaries are established.

**Electronic learning journals for recording children's progress**

* Staff must seek permission from the senior management team prior to using any online learning journal. A risk assessment is completed with details on how the learning journal is managed to ensure children are safeguarded.
* The iPads, Tablets and other image capturing devices that are used by staff to collect images of children, are for the purpose of the Online Learning Journal System and are used for observations and journal entries. They are shared with parents that have an individual account login and account on EyLog, to access, which can be used to access images and videos of their own children only.

**Other Devices with imaging and sharing capabilities.**

It is acknowledged that people may also have other technological devices in their possession or within their personal belongings. This policy is also applicable to other devices with imaging and sharing capabilities, such as:

* Tablets
* Laptops
* Desktop computers with webcams
* Smartwatches with camera features
* Gaming consoles with built-in cameras.
* Digital video recorders (DVRs).
* Drones equipped with cameras.
* Roles and Responsibilities for Parents and Visitors
* Ensure your child(ren) do not bring mobile phones or other ICT devices with them to the setting. If a child is found to have a mobile phone or ICT device with them, this is removed and stored in locked safe until the parent collects them at the end of the session.
* Parents and visitors are requested not to use their mobile phones whilst on the premises. We make an exception if a visitor's company or organisation operates a lone working policy that requires contact with their office periodically throughout the day. Visitors will be advised of a quiet space where they can use their mobile phone, where no children are present.
* Parents and visitors to the nursery that are seen with mobile phones on display whilst moving around the nursery, (during drop off and collection times) will always be asked to remove these from the premises immediately.
* Parents and carers are informed that whilst they can take pictures and videos of their OWN children during a performance these are not to be shared on social media sites and they are for their own personal use. Permission will be sought, prior to any performances, from parents and carers of all children taking part, for agreement to a recording take place i.e. in the event of a nursery video being produced. If permission is denied, then this would be made clear to all parents before the performance took place.
* Compliance and Disciplinary Measures
* All staff, volunteers and students associated with The Little Bumblebee Nursery are expected to adhere to the Online Safety Policy.
* Regular training sessions will be provided to ensure awareness of the policy's guidelines and updates.

*Clear Staff Awareness:*

* Staff members are explicitly informed that the distribution of indecent images is a criminal offence.

*Adherence to Safeguarding Policies:*

* In the event of concerns regarding a colleague or any other person behaving inappropriately, the Safeguarding Policy is followed.

*Reporting Suspicions:*

* Staff members are obligated to report any suspicions of abuse or inappropriate behaviour, including situations involving the use and distribution of inappropriate images. Any concerns or breaches of the policy should be reported promptly to the Designated Safeguarding Lead.

*Legal Obligations:*

* The nursery is committed to adhering to legal obligations related to inappropriate image use, ensuring the safety and well-being of all children in our care.

*Recognition and Reporting of Online Grooming:*

* Staff members are educated on the recognition and reporting of online grooming, understanding that it is an offence.

*Prompt Reporting Procedures:*

* Concerns about the behaviour of a colleague or any other person are promptly reported following established procedures outlined in our Safeguarding policy.

*Disciplinary Measures:*

Breach of this policy may result in disciplinary action up to and including dismissal. Disciplinary action may be taken regardless of whether the breach is committed during working hours, and regardless of whether our equipment or facilities are used for the purpose of committing the breach.

* Any member of staff suspected of committing a breach of this policy will be required to co-operate with our investigation, which may involve handing over relevant passwords and login details.
* Staff may be required to remove internet postings which are deemed to constitute a breach of this policy.
* Failure to comply with such a request may in itself result in disciplinary action. Social media should never be used in a way that breaches any of our other policies. If an internet post would breach any of our policies in another forum, it will also breach them in an online forum. For example, employees are prohibited from using social media to:

1. breach our obligations with respect to the rules of relevant regulatory bodies.
2. breach any obligations they may have related to confidentiality;
3. breach our Disciplinary Rules;
4. defame or disparage the organisation or its affiliates, customers, clients, business partners, suppliers, vendors or other stakeholders.
5. harass or bully other staff in any way or breach our Anti-harassment and bullying policy;\*
6. unlawfully discriminate against other staff or third parties or breach our Equal opportunities policy;
7. breach our Data protection policy (for example, never disclose personal information about a colleague online);
8. breach any other laws or ethical standards (for example, never use social media in a false or misleading way, such as by claiming to be someone other than yourself or by making misleading statements.

*Disciplinary Procedures:*

*First Offense:*

* A verbal warning and reiteration of the online safety guidelines.
* Additional training on responsible online behaviour may be required.

*Second Offense:*

* A written warning highlighting the repeated violation.
* Mandatory attendance at further training sessions.
* Restricted access to certain online privileges within the nursery community.

*Third Offense:*

* Meeting with nursery management to discuss the severity of the violations.
* Temporary suspension of online privileges.
* Further training and reassessment of the individual's commitment to the policy.

*Serious or Repeated Offenses:*

* Immediate suspension or termination of access to nursery online platforms.
* Meeting with nursery management to discuss the consequences and potential reintegration steps.
* In severe cases, legal action may be considered.
* If it is suspected that a staff mobile phone or technological device may contain unsuitable material, the nature of the material should be documented, and the Designated Safeguarding Lead would be informed. The process outlined in the Safeguarding Policy will be followed, including taking advice from external agencies (e.g. police, LADO) as appropriate.

**Online Safety Processes and Procedures**

We take steps to ensure that there are effective procedures in place to protect children, young people and vulnerable adults from unacceptable use of information communication technology [ICT] equipment or exposure to inappropriate materials in the settings.

*1. Risk Assessment:*

* Regularly assess potential risks associated with online activities within the nursery.
* Identify and mitigate risks related to the use of electronic devices, social media, and image sharing.

*2. Training and Awareness:*

* Conduct regular training sessions for staff, parents, and guardians on online safety guidelines. Training for DSL and Staff: The DSL should access training on unique risks associated with online safety, and staff should receive quality and up-to-date online safety training.
* Raise awareness about the potential risks and best practices for maintaining a secure online environment.

*3. User Authentication:*

* Implement secure user authentication processes to control access to online platforms.
* Ensure that only authorized individuals have access to sensitive information.

*4. Data Protection Measures:*

* Establish robust data protection measures in accordance with relevant legislation.
* Safeguard personal information, ensuring secure storage and transmission.

*5. Monitoring and Reporting:*

* Implement monitoring mechanisms to track online activities within the nursery community.
* Establish clear reporting procedures for any concerns or incidents related to online safety.

*6. Communication Channels:*

* Maintain open communication channels between nursery management, staff, parents, and guardians regarding online safety updates.
* Foster a collaborative approach to address any emerging issues promptly.

*7. Incident Response:*

* Management will implement an incident response plan outlining steps to be taken in case of a security breach or violation.
* Establish a designated team responsible for managing and resolving online safety incidents.

*8. Regular Policy Review:*

* Conduct regular reviews of the Online Safety Policy to ensure alignment with evolving technologies and best practices.
* Update processes and procedures as needed to address emerging threats and challenges.

*9. Parental Consent:*

* Obtain explicit parental consent for the use of images and any online activities involving their children.
* Clearly communicate the purpose and nature of online interactions to parents.

*10. Emergency Contact Information:*

* Maintain up-to-date emergency contact information for all children in case of unforeseen online incidents.
* Ensure efficient communication with parents and guardians during emergencies.
* Reporting a Concern

If a parent is worried about the online safety of their child, they can report this to the **DSL**, which will be recorded and actioned. If this is not the case, you may contact ECRIS on 020 8825 8000 or ECIRS@ealing.gov.uk .

If staff become aware that a child is the victim of cyber-bullying, they discuss this with their parents and refer them to sources of help, such as the

* the Internet Watch Foundation (IWF) if settings need to report illegal images (child sexual abuse material). Link: <https://www.iwf.org.uk/>
* the Child Exploitation and Online Protection centre (CEOP) if they are worried about online abuse or the way that someone has been communicating online. Link: <https://www.ceop.police.uk/ceop-reporting/>
* The UK Safer Internet Centre Helpline for Professionals or the NSPCC for further information. Link: <https://www.saferinternet.org.uk/professionals-online-safety-helpline>

If a staff member is concerned about another staff member, they can report this to the DSL, refer to the Whistleblowing Policy and NSPCC whistleblowing helpline.

Link:<https://www.nspcc.org.uk/what-you-can-do/report-abuse/dedicated-helplines/whistleblowing-advice-line/>

* Incident Response Procedure:

**1. Incident Identification:**

* Definition: An incident is any event that compromises the security, integrity, or confidentiality of data or systems.
* Detection Sources: Incidents may be identified through system logs, reports from staff or parents, monitoring tools, or automated alerts.

**2. Initial Response:**

* Designated Person: The Designated Safeguarding Lead (DSL) will be the initial point of contact for reporting security incidents.
* Reporting: Staff should report any suspicious activities or incidents to the DSL immediately.

**3. Triage and Assessment:**

* DSL Responsibilities: The DSL will assess the nature and severity of the incident.
* Documenting: Keep detailed records of the incident, including the date, time, and nature of the security breach.

**4. Containment:**

* Isolation: Take immediate steps to isolate affected systems or areas to prevent further damage or unauthorized access.
* Temporary Measures: Implement temporary measures to limit the impact of the incident.

**5. Eradication:**

* Identify the Source: Determine the root cause of the incident and eliminate it.
* System Updates: Apply necessary updates or patches to prevent a similar incident in the future.

**6. Recovery:**

* System Restoration: Restore affected systems to normal operation.
* Data Recovery: Retrieve and validate any lost or compromised data from backups.

**7. Communication:**

* Internal Notification: Inform relevant staff members about the incident and the steps being taken to address it.
* External Communication: If required, communicate with parents or relevant external parties about the incident, emphasizing the steps taken to resolve it.

**8. Investigation:**

* DSL and IT Staff: Conduct a thorough investigation to determine the extent of the incident, identify vulnerabilities, and gather evidence.
* Legal Considerations: Consult legal counsel if the incident involves potential legal ramifications.

**9. Reporting:**

* Regulatory Reporting: Comply with any legal or regulatory requirements for reporting security incidents.
* Internal Reporting: Provide a comprehensive report to senior management, including findings, actions taken, and recommendations for improvement.

**10. Review and Update:**

* Lessons Learned: Conduct a post-incident review to identify lessons learned and areas for improvement.
* Policy and Procedure Update: Revise the incident response plan and any related policies based on the review.

**11. Support for Affected Individuals:**

* Counseling: Provide counselling or support for individuals (staff, parents, or children) who may be affected by the incident.
* Information Sharing: Keep affected parties informed about the incident and the steps taken to address it.

**12. Continuous Monitoring:**

* Ongoing Monitoring: Implement continuous monitoring of systems and activities to detect and respond to potential future incidents.
* Training: Provide ongoing training to staff on security best practices and incident response procedures.
* Policy Changes
* The safeguarding policies and procedures include all electronic devices with imaging and sharing capabilities, not just mobile phones, and cameras.
* Key Contacts

**Designated Safeguarding Lead**

Mojdeh Najafpoor - Nursery Manager

* Nursery Landline: 020 4501 4097
* Email: [info@little-bumblebee.co.uk](mailto:info@little-bumblebee.co.uk)

In emergencies, contact Mojdeh directly on the provided mobile.

* Mobile: 07463 916 323

**NSPCC**

* Contact: 0808 800 5000
* Website: <https://www.nspcc.org.uk/onlinesafety>

**Childline**

* Contact: 0800 1111
* Website: [www.childline.org.uk](http://www.childline.org.uk).

**ECRIS**

* Contact: 020 8825 8000
* Email: ECIRS@ealing.gov.uk .

**The Internet Watch Foundation (IWF)**

if settings need to report illegal images (child sexual abuse material).

* Link: <https://www.iwf.org.uk/>

**The Child Exploitation and Online Protection centre (CEOP)**

if they are worried about online abuse or the way that someone has been communicating online.

* Link: <https://www.ceop.police.uk/ceop-reporting/>

**The UK Safer Internet Centre Helpline**

* Link: <https://www.saferinternet.org.uk/professionals-online-safety-helpline>

**Whistleblowing Policy and NSPCC whistleblowing helpline**

* Link:<https://www.nspcc.org.uk/what-you-can-do/report-abuse/dedicated-helplines/whistleblowing-advice-line/>

**Policy management and review**

* The Little Bumblebee will review this policy annually. In cases of relevant legal or procedural changes, we will review this policy accordingly. The policy should be made available on the Nursery website, with paper copies provided by the Nursery upon request.
* The policy should be approved, signed and dated and the date for review noted.
* The policy should be provided to and followed by all staff and volunteers.

This policy statement was adopted on 01/01/2023.

|  |  |
| --- | --- |
| Reviewed By: Mojdeh Najafpoor | Date: 02/01/2024 |
| Signed:  A handwritten oval shape with a black line  Description automatically generated with medium confidence | Next Review Date: 02/01/2025 |