**Privacy Policy and Procedure**

Table of Contents

[Introduction 2](#_Toc156232907)

[ Purpose 2](#_Toc156232908)

[ Scope 2](#_Toc156232909)

[ Relevant legislation and guidance 2](#_Toc156232910)

[Data Management 2](#_Toc156232911)

[ Information Collected: 2](#_Toc156232912)

[ Use of Information: 2](#_Toc156232913)

[ Data Sharing: 3](#_Toc156232914)

[ Security Measures: 3](#_Toc156232915)

[Your Rights 4](#_Toc156232916)

[Your Rights: Processes and Procedures 5](#_Toc156232917)

[Privacy Expectations 6](#_Toc156232918)

[ Roles and responsibilities For Staff, Students and Volunteers 6](#_Toc156232919)

[ Compliance and Disciplinary Measures: 7](#_Toc156232920)

[ Roles and responsibilities For Management 8](#_Toc156232921)

[Privacy Processes and Procedures 8](#_Toc156232922)

[ Confidentiality Breach Reporting and Handling: 9](#_Toc156232923)

[Key Contacts: 9](#_Toc156232924)

[Legal Compliance: 10](#_Toc156232925)

[Policy management and review 10](#_Toc156232926)

**Introduction**

Welcome to The Little Bumblebee Limited's Privacy Policy – a guide designed to ensure your confidence and trust in our commitment to safeguarding your privacy. In this document, we outline how we handle your personal information, emphasizing transparency, security, and adherence to data protection regulations. As valued members of our community, your privacy is our priority, and this brief introduction serves as an invitation to explore the details within our official Privacy Policy.

* Purpose

The purpose of this policy is to establish clear guidelines and expectations for maintaining confidentiality and privacy within The Little Bumblebee Nursery. It aims to ensure the protection of sensitive information related to children, families, and staff, reinforcing our commitment to professionalism.

* Scope

This policy applies to all team members, including staff, volunteers, and students, emphasizing the universal responsibility for upholding confidentiality and privacy. It covers all aspects of nursery operations, from enrolment details to internal communications and interactions with families.

* Relevant legislation and guidance
* Statutory Framework for the Early Years Foundation Stage (EYFS) 2023 and related regulations.
* Compliance with the General Data Protection Regulation (GDPR)
* The Freedom of Information Act 2000 regarding data storage and access.

Data Management

* Information Collected:

*Types of Information:*

* Personal Information: Names, addresses, contact details.
* Demographic Information: Age, gender, ethnicity.
* Educational Information: Academic records, school/nursery attended.
* Health Information: Medical history, immunization records.
* Emergency Contact Information: Guardian or emergency contact details.
* Financial Information: Billing details, payment records.
* Media Consent Information: Consent for photography or videography.

We inform parents when we need to record confidential information beyond the general personal information we keep - for example regarding:

* Any injuries,
* Concerns or changes in relation to the child or the family,
* Any discussions with parents on sensitive matters,
* Any records we are obliged to keep regarding action taken in respect of child protection.
* Any contact and correspondence with external agencies in relation to their child.
* Use of Information:

*Purpose of Collecting Information:*

* Child's Well-being: Ensure safety, health, and overall well-being.
* Educational Planning: Tailor education based on individual needs.
* Emergency Situations: Facilitate effective emergency response.
* Communication with Parents: Foster effective parent communication.

*How collected information is utilised.*

* Personalized Care: Provide personalized attention.
* Educational Development: Enhance programs based on academic records. Our staff discuss children's general progress and wellbeing in meetings, but more sensitive information is restricted to our manager and the child's key person and is shared with other staff on a need-to-know basis.
* Health and Safety Measures: Implement measures based on medical history.
* Financial Transactions: Facilitate billing and financial transactions.
* Media Usage: Utilize media consent for documentation.
* Operational Efficiency: Ensure smooth nursery operation with accurate information.
* Data Sharing:

*Circumstances under which information may be shared.*

Information about children and families may be shared under specific circumstances to ensure their well-being and development. Instances include:

* Compliance with legal obligations related to child protection.
* Collaboration with external agencies for the child's educational or developmental needs.
* Emergency situations where sharing information is crucial for the child's safety.

*Third parties with whom information may be shared.*

Information may be shared with specific third parties involved in the child's care and development, including:

* Educational authorities overseeing compliance and quality standards.
* External service providers supporting the nursery's operations.
* Collaborative partners engaged in educational initiatives.
* Authorized individuals or entities as required by law, such as legal representatives or safeguarding authorities.
* Security Measures:

**Steps taken to safeguard collected information:**

*Physical Security:*

* Information stored in physical form is kept in secure and locked cabinets accessible only to authorized personnel.
* Restricted access to areas where physical records are maintained ensures additional protection.

*Digital Security:*

* Electronic records are stored on password-protected computers within a secure, locked room in the nursery office.
* Regularly updating and maintaining strong, unique passwords for all digital access points.

*Access Control:*

* Implementing access control measures to restrict information access to authorised staff members only.
* Conducting periodic reviews to ensure access permissions align with job responsibilities.

**Security protocols in place:**

* *Encryption:* Utilizing encryption methods for transmitting sensitive information to maintain confidentiality during data exchange.
* *Regular Audits:* Conducting routine security audits to identify vulnerabilities and address any potential risks promptly.
* *Staff Training:* Providing ongoing training to staff on security protocols and the importance of maintaining confidentiality.
* *Incident Response Plan:* Establishing a clear incident response plan to address and mitigate the impact of any security breaches promptly.
* *Secure Communication:* Ensuring secure communication channels for any information sharing, especially sensitive or confidential data.

**Your Rights**

This section outlines the rights individuals possess regarding their personal information, emphasizing our commitment to transparency, control, and respect for privacy. Here, we elucidate the options available for individuals to manage their information and the procedures for exercising these fundamental rights.

*Access to Personal Information:*

* Individuals have the right to request access to the personal information held about them by The Little Bumblebee Nursery.
* Upon request, the nursery will provide details on the types of information collected and the purposes for which it is used.
* If there are any controversial aspects of the content of a child's file, we must seek legal advice. This might be where there is a court case between parents, where social care or the police may be considering legal action, or where a case has already completed, and an appeal process is underway.

*Correction of Information:*

* The law requires that the information we hold must be held for a legitimate reason and must be accurate (see our Privacy Notice). If a parent says that the information, we hold is inaccurate, then the parent has a right to request for it to be changed. However, this only pertains to factual inaccuracies.
* Where the disputed entry is a matter of opinion, professional judgement, or represents a different view of the matter than that held by the parent, we retain the right not to change that entry, but we can record the parent's view of the matter. In most cases, we would have given a parent the opportunity at the time to state their side of the matter, and it would have been recorded there and then.

*Withdrawal of Consent:*

* Individuals have the right to withdraw their consent for the processing of personal information.
* The nursery will respect such requests, and individuals will be informed of the potential consequences of withdrawing consent.

*Data Portability:*

* Individuals have the right to receive their personal information in a structured, commonly used, and machine-readable format.
* The nursery will facilitate the transfer of relevant data upon request.

*Objection to Processing:*

* Individuals can object to the processing of their personal information based on specific grounds.
* The nursery will assess and accommodate such objections unless there are compelling legitimate grounds for processing.

*Restriction of Processing:*

* Individuals may request the restriction of processing their personal information under certain circumstances.
* The nursery will limit processing activities during the assessment of such requests.

*Right to Complain:*

* If a parent feels aggrieved about any entry in the file, or the resulting outcome, then we refer the parent to our Complaint’s Policy and Procedures.

*Parent-to-Parent Sharing:*

* Some parents may choose to share information about themselves with fellow parents as well as our staff.
* The nursery cannot be held responsible if shared information is disclosed by those parents to whom you have confided. We encourage open communication and trust among parents while also emphasizing the importance of individual responsibility in maintaining confidentiality.

**Your Rights: Processes and Procedures**

Where third parties share information about an individual us; our practitioners and managers check if it is confidential, both in terms of the party sharing the information and of the person whom the information concerns. Parents may request access to any confidential records we hold on to their child and family following the procedure below:

**Parental Access Request Procedure:**

* The parent is the 'subject' of the file in the case where a child is too young to give "informed consent' and has a right to see information that our setting has compiled on them.
* Any request to see the child's personal file by a parent or person with parental responsibility must be made in writing to the setting leader or manager/Director.
* We keep copies of these letters and their replies on the child's file.

Parents may request access to any confidential records we hold on to their child and family, following this procedure:

1. *Request Submission:*

* Requests to access the child's personal file must be made in writing to the setting leader or manager/Director.
* Copies of these request letters and their replies are maintained on the child's file.

1. *Acknowledgment and Arrangement:*

* We acknowledge the request in writing, assuring the parent that arrangements will be made for them to see the file contents, subject to third-party consent. We will be able to extend this by a further two months where requests are complex or numerous. If this is the case, we will inform you within one month of the receipt of the request and explain why the extension is necessary.

1. *Fee Consideration:*

* A fee may be charged for repeated requests, or where a request requires excessive administration to fulfil.

1. *Managerial Actions:*

* The manager and their deputy manager go through the file, ensuring correct filing, date order, and no missing pages.
* Any information, entry, or correspondence mentioning a third party is duly noted.

1. *File Review:*

* Our manager goes through the file with their deputy manager and ensures that all documents have been filed correctly, that entries are in date order and that there are no missing pages. They note any information, entry or correspondence or other document which mentions a third party.

1. *Notification to Third Parties:*

* We write to each of those individuals explaining that the subject has requested sight of the file, which contains a reference to them, stating what this is.
* They are asked to reply in writing to our manager giving or refusing consent for disclosure of that material.

1. *Consent from Third Parties:*

* Third parties include each family member noted on the file; so where there are separate entries pertaining to each parent, step parent, grandparent etc. we write to each of them to request third party consent.
* Third parties also include workers from any other agency, including children's social care and the health authority for example. Agencies will normally refuse consent to share information, preferring instead for the parent to be redirected to those agencies for a request to see their file held by that agency.

1. *Staff Communication and Sensitivity Consideration:*
   * Members of our staff should also be written to, but we reserve the right under the legislation to override a refusal for consent or to just delete the name of the staff member and not the information. We may grant refusal if the member of staff has provided information that could be considered "sensitive' and the staff member may be in danger if that information is disclosed; or if that information is the basis of a police investigation. However, if the information is not sensitive, then it is not in our interest to withhold that information from a parent. In each case this should be discussed with members of staff and decisions recorded.
2. *Copy Preparation and Legal Verification:*
   * When we have received all the consents/refusals our manager takes a photocopy of the complete file. On the copy of the file, our manager removes any information that a third party has refused consent for us to disclose and blank out any references to the third party, and any information they have added to the file, using a thick marker pen.
   * The copy file is then checked by [the deputy manager and] legal advisors to verify that the file has been prepared appropriately.
   * What remains is the information recorded by the setting, detailing the work initiated and followed by them in relation to confidential matters. This is called the clean copy.
3. *Communication with the Parent and Review Meeting:*
   * We photocopy the 'clean copy' again and collate it for the parent to see.
   * Our manager informs the parent that the file is now ready and invite's him/ her to make an appointment to view it.

* Our manager and their line manager meet with the parent to go through the file, explaining the process as well as what the content of the file records. To ensure it is properly explained to and understood by the parent, we never hand it over without discussion. Only the person(s) with parental responsibility can attend that meeting, or the parent's legal representative or interpreter may request information about the child and the work that has been done.
  + Information shared with other agencies is done in line with our Information with the setting's Information Sharing Policy.

**Privacy Expectations**

* Roles and responsibilities For Staff, Students and Volunteers

*Confidentiality Agreement:*

* + Staff should refrain from discussing nursery matters outside the premises.
  + Discussions about a child must involve the child's parents, authorized carer, or fellow nursery staff.
  + Safeguard information about children and families, restricting discussions to necessary professional contexts within the nursery setting.
  + All staff members sign a confidentiality agreement upon commencing employment.
  + Respect the privacy of colleagues by refraining from discussing personal matters outside the professional realm.
  + Information sharing within the staff team occurs on a 'need-to-know' basis and is treated with utmost confidentiality.

*Children and Families:*

* + Information about children and families is strictly confidential and should not be discussed outside necessary professional conversations within the nursery setting.

*Colleague Information:*

* + Respect the privacy of colleagues by refraining from discussing personal information outside the professional context of work.

*Nursery Operations:*

* + Operational details, internal communications, and discussions regarding nursery policies and procedures should be kept confidential.
* Recognizing the sensitive nature of information, it is used for specific purposes, such as meeting children's needs, maintaining registers, handling invoices, and managing emergency contacts.
* Information is stored securely, adhering to data protection principles.

*Media and social media:*

* + Refrain from sharing nursery-related content on personal or public social media accounts without explicit consent, respecting the privacy of children and families.

*Record-Keeping:*

* + Maintain accurate and secure records with limited access to authorized personnel.
  + It is an offense to remove controversial material or rewrite records to make them more acceptable.

*Disclosures:*

* + Report concerns or disclosures about the well-being of a child or colleague to the designated Safeguarding Officer.
  + Sharing such information beyond designated channels is strictly prohibited and may result in disciplinary action.

*Leaving the Nursery:*

* Confidential information remains confidential even after leaving employment.
* Compliance and Disciplinary Measures:

*Handling Date:*

* Staff members are responsible for familiarizing themselves with the privacy policy and ensuring strict compliance.
* Handle personal data with care, following established procedures outlined in the privacy policy.
* Continuous training is essential for staying informed about privacy regulations and best practices.

*Training and Awareness:*

* Comprehensive training and awareness programs will be provided regularly to ensure familiarity with the Confidentiality Policy.

*Monitoring and Auditing:*

* Regular monitoring and auditing of compliance with the Confidentiality Policy, including reviewing access logs and assessing adherence to procedures.

*Confidentiality Agreement:*

* All staff members are required to sign a Confidentiality Agreement, and failure to adhere may result in disciplinary action.

*Reporting Violations:*

* Individuals aware of violations must promptly report incidents to designated authorities.

*Confidentiality Breach Investigation:*

* Thorough investigation in the event of a breach to determine its extent, identify the responsible party, and assess potential impact.

*Disciplinary Measures:*

* Non-compliance may result in disciplinary action, ranging from verbal warnings to termination of employment.

*Appeals Process:*

* Staff have the right to appeal disciplinary actions, ensuring a fair and impartial review.

*Continuous Improvement:*

* Lessons learned from breaches will be used for continuous improvement in policies, procedures, and training.

*Legal Consequences:*

* Breaches may have legal consequences, and individuals may face legal action for intentional or grossly negligent violations.

*Confidentiality Violation Records:*

* Records of violations and corresponding disciplinary actions will be securely stored in compliance with data protection regulations.
* Roles and responsibilities For Management
* Uphold the highest standards of confidentiality and implement robust security measures.
* Collect and process only necessary data for the intended purpose, minimizing personal information handled.
* Clearly define the purpose for collecting and processing personal data, ensuring alignment with lawful objectives.
* Obtain informed and explicit consent, communicating transparently about data usage.
* Strive for accuracy and maintain up-to-date personal information.
* Retain data only for the necessary duration, disposing of it securely.
* Respect and facilitate the exercise of individuals' rights regarding their personal data.
* Ensure data integrity and confidentiality through preventive measures.
* Establish accountability mechanisms and regularly assess adherence to the privacy policy.
* Commit to continuous improvement, reviewing and updating the policy as needed.
* Ensure third parties adhere to the same privacy standards and security measures.
* Operate in compliance with relevant privacy laws, taking proactive measures to adapt to legal requirements.

**Collective Responsibility:**

* Report any potential breaches or concerns regarding privacy promptly to designated authorities.
* Foster a culture of privacy and data protection within the organization.
* By delineating clear roles and responsibilities, this ensures a unified effort among staff, students, and volunteers to uphold the privacy standards outlined in the policy.

**Privacy Processes and Procedures**

*Privacy Respect:*

* Confidential records are stored securely, ensuring access is restricted to authorized personnel.
* Staff, student, and volunteer inductions emphasize the importance of confidentiality.

*Awareness and Respect:*

* All individuals associated with the nursery, including students on placement, are made aware of and expected to respect the confidentiality policy.

*Parental Access:*

* Parents have access to their own children's files and records but not to those of other children, unless authorized by relevant professionals in specific circumstances (See Privacy Policy).

*Consent Requirement:*

Any request for confidential information, for whatever reason, requires parental permission.

* Internal Communication:
* Staff are prohibited from discussing personal information provided by parents with other staff members, except when relevant to planning for the child's needs.

*Employment Matters:*

* Issues related to staff employment remain confidential among those directly involved in personnel decisions.

*Child Safety Concerns:*

* Concerns or evidence related to a child's personal safety are kept in a secure, confidential file and shared only with individuals on a 'need-to-know' basis, prioritizing the child's best interests as per our safeguarding/child protection policy.

**Guidelines for Digital Communications and Electronic Information:**

*Social Networking Policy:*

* + Staff, students, and volunteers must adhere to the social networking policy to maintain confidentiality.
  + Staff, students, and volunteers are prohibited from sharing photographs of or information about children on their personal accounts.

*Secure Communication Platforms:*

* Team members must use secure communication channels and platforms when discussing or transmitting confidential information.
* Adherence to established guidelines ensures the confidentiality of digital communications.

*Encryption and Secure Storage:*

* Electronic information containing confidential data will be encrypted and stored securely on password-protected devices and servers.
* Secure transmission protocols will be employed to protect data during electronic transfer.

**Guidelines for Discussing and Handling Confidential Matters:**

*Authorized Contexts:*

* Discussions involving sensitive or confidential matters should occur within designated and authorized contexts, such as team meetings or designated office spaces.
* Team members are reminded to exercise discretion and professionalism in all discussions.

*Restricted Disclosures:*

* Team members are prohibited from discussing sensitive information outside of designated and authorized contexts.
* Adherence to these limits ensures the preservation of confidentiality and trust within the nursery community.
* Confidentiality Breach Reporting and Handling:

*Reporting Process:*

* Team members are required to promptly report any suspected or actual confidentiality breaches to their immediate supervisor or designated authority.
* The reporting process ensures timely identification and assessment of breaches.

*Investigation and Resolution:*

* Reported breaches will be thoroughly investigated to determine the extent and nature of the incident.
* The nursery will take appropriate corrective actions to address breaches and prevent future occurrences.

*Incident Documentation:*

* All confidentiality breaches and related incidents will be documented, detailing the circumstances, individuals involved, and actions taken.
* Comprehensive documentation ensures transparency and accountability in addressing breaches.

Key Contacts:

**Designated Contact - Nursery Manager:**

For any inquiries or concerns related to confidentiality, individuals may contact the Nursery Manager directly.

Email: info@little-bumblebee.co.uk

Phone: 020 4501 4097

Legal Compliance:

*Commitment to Data Protection Laws:*

* The organization, The Little Bumblebee Limited, hereby acknowledges its unwavering commitment to complying with all relevant data protection laws.

*Incorporation of Legal Framework:*

* This policy aligns with and adheres to the provisions set forth by existing data protection laws, including but not limited to the General Data Protection Regulation (GDPR) and the Freedom of Information Act 2000.
* The organization ensures that its practices and procedures are in accordance with the statutory framework for the Early Years Foundation Stage (EYFS) 2023 and related regulations governing the collection, storage, and processing of personal information.

**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 01/02/2023.

|  |  |
| --- | --- |
| 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 |