Howe Dell Day Care

Confidentiality Policy

Policy adopted in August 2007, to be reviewed May 2027

Aim

At Howe Dell Day Care, we are committed to upholding the highest standards of confidentiality across all aspects of our practice. This policy ensures that no information, whether verbal, written, or digital will be disclosed to any unauthorised individuals or organisations regarding any child who is currently, or has previously been, enrolled in our setting.

Our aim is to protect the privacy of children, families, and staff by ensuring all shared information is handled with sensitivity, respect, and in full compliance with our legal and professional responsibilities. We are dedicated to maintaining trust, safeguarding children, and meeting the requirements set out in the Early Years Foundation Stage (EYFS) Framework**,** UK General Data Protection Regulation (UK GDPR)**,** and other relevant legislation.

Procedures

To uphold confidentiality within the setting, the following procedures are implemented:

- **Right to Privacy:** Every child, family, and staff member has the right to privacy.
- **Respect for Information:** All information shared with the setting is treated with sensitivity, discretion, and respect.
- **Scope of Confidentiality:** Confidentiality applies to all forms of communication, including written records, verbal discussions, emails, photographs, and digital files.
- **Legal Compliance:** The setting complies fully with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, and, where applicable, the Freedom of Information Act 2000.
- **Secure Information Handling:** Personal data is securely stored and only accessible to authorised personnel.

- **Staff Responsibility:** All staff, students, and volunteers are expected to follow confidentiality procedures as part of their professional conduct.

- **Parental Communication:** Personal or sensitive information is only shared with parents/carers when it relates directly to their own child, unless legally required or in safeguarding situations.

Staff Conduct

To maintain high standards of confidentiality and professionalism, all staff must:

Refrain from discussing individual incidents or a child's behaviour in the presence of other parents, carers, or children.

Only discuss personal information shared by parents when it directly impacts planning or provision for that child's care, learning, or development.

Never share personal details unless exceptional circumstances arise that justify disclosure in accordance with legal requirements or safeguarding obligations.

Staff Responsibilities

To ensure consistency and compliance with confidentiality procedures:

All staff, students, and volunteers are introduced to the confidentiality policy as part of their induction process.

Staff must not discuss any individual child, family, or colleague outside the professional context of the setting.

Staff must not share information with other parents or carers under any circumstances.

All staff are expected to always model respectful and responsible handling of sensitive information.

Data Storage and Access

All records, documentation, and personal data relating to children, families, and staff are stored securely, whether in paper or electronic format.

Access to such records is restricted to authorised staff members only and is granted solely on a need-to-know basis in line with their professional responsibilities.

Confidential documents are stored in locked filing cabinets or secure digital systems protected by passwords and encryption where applicable. Please refer to E Safety policy.

Data Protection

Howe Dell Day Care and School is fully compliant with the UK General Data Protection Regulation (UK GDPR) and the Freedom of Information Act 2000.

The setting is registered as a Data Controller with the Information Commissioner's Office (ICO).

All staff are made aware of their responsibilities under data protection legislation during induction and receive regular training updates as needed.

Parental Access

Parents and carers may request access to records relating to their own child. All requests must be submitted in writing to the setting manager or designated data protection lead.

Access will be granted in accordance with data protection legislation and within appropriate timescales.

Under no circumstances will information about other children, families, or individuals be disclosed. This ensures we maintain the confidentiality and privacy of all families within the setting.

Social Media and Professional Boundaries

All staff receive training on maintaining confidentiality, including the responsible use of social media and networking platforms.

Staff must not share any identifiable, sensitive, or personal information relating to children, families, colleagues, or the setting on social media or any public or private online platform.

Staff are expected to maintain professional boundaries online and refrain from discussing work-related matters in any informal digital context.

Electronic and Digital Security

All digital records are stored on secure, password-protected systems accessible only to authorised personnel.

Staff are strictly prohibited from storing or sharing sensitive information on personal devices or through non-approved communication channels.

Photographs or videos of children will only be taken and used in accordance with written parental consent and the setting's Image Use Policy.

Staff must follow data handling protocols when accessing or transferring digital files to prevent unauthorised access or data breaches.

Information Sharing Responsibility

Information Handling

Personal records, such as registration forms, child development records, and medical information, are stored securely and accessed only by authorised personnel.

Personal information shared by parents or carers is used solely to support the care, learning, and development of their child.

All records are retained and disposed of in accordance with the setting's Data Retention Policy and relevant legal and regulatory guidance.

While parents/carers may choose to share personal information with others, Howe Dell Day Care and School cannot be held responsible for the sharing or circulation of such information outside our staff team.

Safeguarding Exception

In situations where a member of staff suspects that a child may be at risk of abuse or neglect, the Safeguarding and Child Protection Policy overrides this Confidentiality Policy.
In such cases, information will be shared on a need-to-know basis only, and in full compliance with safeguarding protocols and statutory guidance. In such cases:

Information will be shared with appropriate agencies (e.g. Local Authority Designated Officer, MASH, Social Services) on a need-to-know basis.

Staff must follow the setting's safeguarding procedures and report concerns to the Designated Safeguarding Lead (DSL) immediately.

Students and Volunteers

All students and volunteers are introduced to the Confidentiality Policy as part of their induction process.

They are expected to strictly adhere to the principles and procedures outlined in this policy for the duration of their placement or time within the setting.

Students and volunteers must not share any personal information about children, families, staff, or the setting either inside or outside of the setting, including on social media or with peers.

Breaches of confidentiality may result in the termination of their placement and, where appropriate, reporting to their training provider or other relevant authority.

Monitoring and Review

This policy is reviewed regularly and updated in line with changes to legislation, statutory guidance, or best practice within the early years sector.

All staff are required to familiarise themselves with the policy and will be informed of any updates or revisions.

Ongoing training and discussion form part of our approach to ensuring everyone understands and complies with confidentiality expectations.

Breaches of Confidentiality

Any breach of confidentiality by a staff member, student, or volunteer will be treated as a serious matter.

Breaches may result in disciplinary action, termination of employment or placement, and, where necessary, reporting to external regulatory or professional bodies.

Each incident will be investigated in line with the setting's disciplinary procedures and safeguarding responsibilities.