ROMPERS PRIVATE NURSERY
CONFIDENTIALITY POLICY

Policy Statement:

Rompers Private Nursery is committed to maintaining the highest standards of confidentiality, professionalism, respect and integrity in all aspects of our service. We recognise that families place their trust in us to safeguard personal information and to treat children, parents, carers and colleagues with dignity and respect at all times.

This policy sets clear expectations for staff behaviour both within the setting and outwith the setting, including in public spaces, online environments and private conversations. Staff must ensure that their conduct protects the reputation of the service, the privacy of families, and complies fully with:
- Scottish Social Services Council (SSSC) Codes of Practice
- Care Inspectorate expectations and quality standards
- Data Protection legislation
- GIRFEC and SHANARRI wellbeing indicators

Any breach of confidentiality or unprofessional conduct may place children and families at risk and may result in disciplinary action, referral to the SSSC, or regulatory action.
This policy applies to all employees, students, volunteers, contractors and visitors where relevant and applies both inside and outside working hours.

UNCRC Articles: 12, 16, 42

Aims of this Policy:

- Children and families feel safe, respected and confident in how their information is handled.
- Staff clearly understand their responsibilities regarding confidentiality and professional conduct.
- Information is shared appropriately, lawfully and only when necessary.
- The integrity and reputation of Rompers Private Nursery is protected at all times.
- Staff comply with professional responsibilities under SSSC and Care Inspectorate standards.

Confidential Information - Includes personal details, learning records, safeguarding information, medical needs, family circumstances and internal operational information.

Information Sharing - Information is shared only where lawful, necessary and appropriate. Digital systems must be used securely, and passwords must never be shared.

Procedures:

Access to Information and Records

- Personal and emergency contact information is stored securely within the nursery office and on a secure online system. Access is restricted to Management, Team Leaders and relevant qualified practitioners only.
- Emergency contact details may be accessed via the secure online system and T-cards stored within the office.
- All children have an online learning journal via the platform Ovivio, and Pre-school children also have a physical learning journal folder. Access is controlled to ensure confidentiality and respect for families.
- Children's personal information will not be shared with external parties without parental consent unless safeguarding or legal requirements apply.
- Information from MyWorld documentation will be shared with other professionals to support the child's learning and development.
- Personal details are reviewed and updated accordingly 6 monthly during MyWorld meeting reviews.
- All students and volunteers receive confidentiality guidance during induction and must comply fully.

Information Sharing Within the Setting

- Information is shared with staff on a strict need-to-know basis only, staff must respect this in a professional manner.
- Information shared by parents must not be discussed across rooms or communal areas.
- Discussions about children are limited to professional purposes only, staff are only permitted to share their professional viewpoint.

Professional Conduct Outwith the Setting

Staff are representatives of Rompers Private Nursery at all times, including outside working hours, in public spaces, private conversations, and online environments. Professional boundaries must be maintained at all times.

Employees must NOT:

- Discuss any aspect of the nursery, children, families, colleagues, internal matters or incidents with anyone outside the organisation, including former employees, friends, family members or members of the public.
- Engage in gossip, speculation, opinion-sharing or negative commentary about children, families, colleagues or management, whether in person, by telephone, messaging apps or social media.
- Share opinions, judgements or personal views about families, parenting, home circumstances or behaviours outside of appropriate professional discussions within the workplace.

- Disclose information learned through their role, even if they believe the information is anonymous, insignificant or already known by others.
- Participate in conversations that undermine the reputation, integrity or professionalism of the service.
- Discuss operational matters, staffing issues, incidents, complaints or internal decisions with anyone who does not have a legitimate professional need to know.

Employees MUST:

- Maintain respectful, neutral and professional language when referring to the service, families and colleagues at all times.
- Challenge inappropriate conversations or remove themselves from situations where confidentiality or professionalism is being compromised.
- Report any concerns about breaches of confidentiality or unprofessional conduct to management.
- Understand that behaviour outside of working hours can impact professional suitability, SSSC registration and the reputation of the service.

Any breach of this section will be treated as a serious matter and may result in disciplinary action, including referral to the SSSC where appropriate.

Safeguarding and Child Protection

Rompers Private Nursery has a statutory duty to safeguard and promote the welfare of all children. Safeguarding information is highly sensitive and must be handled with the highest levels of confidentiality, professionalism and care at all times. Safeguarding responsibilities override all other considerations, however confidentiality must still be respected and information must only be shared appropriately and lawfully.

Employees MUST:

- Report any safeguarding concern, disclosure, observation or allegation immediately to the Designated Child Protection Co-ordinator or management in line with the Child Protection Policy.
- Record safeguarding information accurately, factually and promptly, using the agreed recording systems and procedures.
- Share safeguarding information strictly on a need-to-know basis and only with authorised professionals.
- Treat all safeguarding information with sensitivity, respect and professional discretion at all times.
- Follow all instructions given by management or external agencies in relation to safeguarding matters.
- Secure any written or digital safeguarding records immediately after use and ensure they are not left unattended or accessible to unauthorised persons.
- Maintain a calm, respectful and non-judgemental approach when dealing with children and families involved in safeguarding matters.

- Seek guidance immediately if unsure how to manage or share safeguarding information.

Employees Must NOT:

- Discuss safeguarding concerns, suspicions, incidents or cases with colleagues who are not directly involved or authorised.
- Share safeguarding information with friends, family members, former staff, or any unauthorised person under any circumstances.
- Speculate, gossip, share opinions or make assumptions about safeguarding matters, families or outcomes.
- Attempt to investigate concerns independently or seek additional information outside of agreed procedures.
- Access safeguarding files or records unless authorised and required for their role.
- Retain copies, notes, photographs or screenshots of safeguarding information on personal devices or outside secure systems.
- Delay reporting a safeguarding concern for any reason.

Storage and Security of Safeguarding Information

- All safeguarding files are stored securely in locked cabinets or protected digital systems with restricted access.
- Access to safeguarding records is limited to identified authorised staff only.
- Safeguarding information must never be removed from the premises or shared electronically unless authorised and secure.
- Digital safeguarding records must be password protected and accessed only on approved devices.

Staff Records and Digital Systems

Rompers Private Nursery uses secure digital systems including Ovivio, Dropbox and Google Calendar to support the safe and effective operation of the service. Access to these systems is granted strictly based on role, responsibility and business need. All staff must understand that access to these systems is a position of trust and must be used professionally, ethically and lawfully at all times.

Employees MUST:

- Access only the information that is necessary for their role and duties. Staff must not access records, documents or calendars out of curiosity or personal interest.
- Use all digital systems solely for legitimate work purposes and in line with nursery policies, data protection legislation, SSSC Codes of Practice and Care Inspectorate expectations.
- Keep login details confidential at all times. Passwords must never be shared, written down, saved on personal devices or disclosed to any other person.

- Log out of systems when not in use and ensure screens and devices are secured to prevent unauthorised access.
- Immediately report any suspected data breach, unauthorised access, lost devices or security concerns to management.
- Handle all information viewed on Ovivio, Dropbox and Google Calendar with strict confidentiality and professional discretion.
- Use professional language and accuracy when recording or sharing information on digital systems.

Employees Must NOT:

- Share, discuss, screenshot, photograph, forward or copy any information accessed through Ovivio, Dropbox or Google Calendar with anyone who does not have authorised access.
- Share information from digital systems with former staff, friends, family members or any third party under any circumstances.
- Use personal devices including phones and watches, messaging apps, email accounts or social media to transmit nursery information unless agreed with Management (Team Leader/Nursery WhatsApp for emergency and information sharing).
- Access records relating to children, families or staff unless directly required for their role.
- Download, store or retain nursery information on personal devices or personal cloud storage.
- Use information obtained through digital systems for personal purposes, opinion-sharing, gossip or discussion outside of professional settings.
- Attempt to bypass security controls, access restricted areas, or use another person's login credentials.

Confidentiality During Leave and After Employment

All confidentiality, safeguarding and professional conduct responsibilities continue to apply during any period of absence from the workplace and after employment has ended. Other staff continuing with employment and not on leave must comply with the following also.

This includes, but is not limited to:

- Maternity/Paternity leave
- Adoption leave
- Sickness absence
- Annual leave
- Career breaks
- Secondments
- Suspension
- Working notice
- Resignation or termination of employment

Access to information and professional obligations remain governed by this policy, SSSC Codes of Practice and data protection legislation.

Employees MUST:

- Maintain strict confidentiality regarding all information learned through their role, regardless of employment status or leave arrangements.
- Continue to uphold professional standards and respectful conduct when referring to the nursery, children, families or colleagues.
- Immediately return or securely delete any nursery property, documents, devices, login access or information when instructed by management.
- Ensure no nursery information is stored on personal devices, personal email accounts or personal cloud storage.
- Direct any requests for information from third parties to management.
- Inform management immediately if they become aware of any accidental retention or access to nursery information during leave.

Employees Must NOT:

- Access nursery systems (including Ovivio, Dropbox, Google Calendar or any internal platforms) unless explicitly authorised by management.
- Discuss nursery matters, children, families, colleagues, safeguarding information or operational matters with anyone outside authorised professional channels.
- Share opinions, speculation or commentary relating to the service, families or staff.
- Retain, copy, screenshot, forward or store any nursery information after access has been removed.
- Use knowledge gained through employment for personal purposes or discussion.

Access Management During Leave and After Employment:

- System access may be restricted, suspended or removed during periods of leave or immediately upon termination of employment.
- Any authorised access during leave will be strictly limited and monitored.
- All keys, devices, and access credentials must be returned as directed by management.

Monitoring, Compliance and Enforcement

Rompers Private Nursery is committed to ensuring that confidentiality, safeguarding and professional conduct standards are consistently upheld across the service.

Compliance with this policy will be actively monitored through:

- Staff induction and ongoing training
- Supervision and appraisal processes

- Audits of record keeping and digital system access
- Observation of professional conduct and practice
- Review of incidents, complaints and concerns

All staff are responsible for understanding and complying with this policy and must seek clarification where uncertainty exists. Ignorance of policy requirements will not be accepted as an excuse for non-compliance.

Any concerns regarding breaches of confidentiality, inappropriate conduct, misuse of information or failure to follow procedures must be reported immediately to management.

Breaches and Enforcement

Breaches of this policy will be taken seriously and investigated promptly, fairly and consistently.

Depending on the nature and severity of the breach, actions may include:

- Informal or formal management action
- Additional training or supervision
- Disciplinary procedures up to and including dismissal
- Restriction or removal of system access
- Referral to the SSSC
- Notification to regulatory or safeguarding authorities where required

Where a breach places a child, family, staff member or the service at risk, immediate protective action will be taken.

Policy Review and Monitoring

This policy will be reviewed annually or sooner where:

- Legislation or statutory guidance changes
- Regulatory requirements change
- Practice concerns or incidents highlight the need for review
- Organisational systems or processes change

Staff will be informed of any updates and are required to comply with the most current version of this policy.

Review

Date	Management	Track of Changes
August 2021	P. Guthrie	none
February 2022	P. Guthrie	Updates to information sharing including MyWorld permissions.
December 2022	TL	Update to procedure: can only be accessed by Management, Team Leaders and Room Champions. T-cards Stored in the office
February 2023	Room Champions	UNCRC articles added
September 2024	TL	None.
December 2024	TL	Update to procedure: Parents emergency contacts can be accessed by qualified practitioners Dropbox
January 2026	K.Waghorn	Update to match current best practice and HR standards.