CHELSEA PRE-PREP

KINGSLAND PRE-PREP

GRAND WEST PRE-PREP

General Data Protection Regulation (UK GDPR) Policy

Table of Contents

General Statement

The General Data Protection Regulation (GDPR) is designed to protect the privacy of individuals. It requires that any personal information about an individual is processed and stored securely and confidentially. This applies to the data of children, parents/carers and staff at the setting. Everybody associated with our Rocket Pre-Preps, has the right to know what information concerning them is used and why, they also have the right to access this information. By complying with the general data protection regulation legislation when processing personal information, we will ensure every individual's privacy is protected.
We aim to ensure that all parents and carers can share their information in the confidence that it will only be used to enhance the welfare of their children under the Early Years Foundation Stage Statutory Framework Requirements (last updated in 2021). Our record keeping systems, means of storing and information sharing take place within the framework of the General Data Protection Regulation and the Human Rights Act.

The principles of GDPR

There are principles of GDPR which we must follow in order to meet the regulations. Article 5 of the GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e. kept in a form which permits identification of data subjects for no longer than is necessary (see data audit for more information) for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest,

scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Our Rocket Pre-preps will only collect data from individuals we have legitimate grounds to do so and will be transparent in the way that we retain and process this information. We will only handle personal information in a lawful and appropriate way, not in a way that could have an adverse effect on the individual, including parents, carers and children.

Sensitive personal data

GDPR provides a separate definition for "sensitive personal data". This relates to information concerning a data subject's racial or ethnic origin, political opinions, religious beliefs, trade union activities, physical or mental health or details of criminal offences. Sensitive personal data is given greater protection as individuals have the right and would expect their personal data to remain private. For instance, our Local Authority Kensington and Chelsea, will ask parents to fill in a confidential ethnicity questionnaire as part of the Early Years National Funding Formula.

Certain personal data is made available by our Rocket Pre-Preps, such as the staff individual email addresses. This is made available for a channel for staff and parents to communicate. We make a distinction between the type of personal data that is appropriate to be shared (as previously mentioned) and personal data that should remain private. For instance, staff personal emails would be expected to remain private, whereas staff's school emails addresses can be shared with parents.

The following is a list of the type of data we hold and process at all our Rocket Pre-Preps, this data is mostly hold as a legal requirement of the EYFS Statutory Framework, legal requirement by HMRC or a legitimate interest. We have a comprehensive list of all the data we hold and why, how and for how long we store it. This can be access by parents and staff in the school Office.

As a general rule, we are required under legislation, subject to the laws relating to data protection and document retention, to keep certain records about children, parents and also staff members for the following set amount of time:

- Children's records - A reasonable period of time after children have left the provision. We will follow the Local Authority procedure here and this states they should be kept for 2 years as stated by Ofsted on the Registration requirements.

- Records relating to individual children e.g. care plans, speech and language referral forms – We will pass these on to the child's next school or setting following our Local Authority's protocols for transition and sharing of sensitive records.
- Copies will be kept for a reasonable period. We will follow the Local Authority procedure here and this states they should be kept for 2 years as stated by Ofsted on the Registration requirements.

- Accidents and pre-existing injuries - If relevant to child protection we will keep these until the child reaches 25 years old.

- Safeguarding Records and Cause for Concern forms – We will keep until the child has reached 25 years old.

- Records of any reportable death, injury, disease or dangerous occurrence (for children) - As these incidents could result in potential negligence claims, or evolve into a more serious health condition, we keep records until the child reaches the age of 21 years and 3 months.

- Records of any reportable death, injury, disease or dangerous occurrence (for staff) – 3 years

- Type of accidents include fractures, broken limbs, serious head injuries or where the child is hospitalised.

- Observation, planning and assessment records of children - We keep our planning filed since the last inspection date so there is a paperwork trail if the inspector needs to see it.

- Information and assessments about individual children is either given to parents when the child leaves or to the next setting/school that the child moves to (with parents' permission).

- Personnel files and training records (including disciplinary records and working time records) – 7 years

- Visitors/signing in book – Up to 24 years as part of the child protection trail.

List of data - overview

Document	Data Recorded	Lawful / Legal Basis for Recording Data	Data Sharing
Accident, Injury and First Aid recording	Child's personal information, Staff names and Parent name and signature	Legal obligation Requirement of statutory framework: EYFS and Childcare Register (Ofsted)	On Request with other agencies- eg. Ofsted, LSCB, LA, GP, HV or Emergency Services
Accounts / HMRC	Invoices for parents, Child's name and booked in sessions, Business expenses including purchase receipts	Legal obligation required by HMRC	On request by HMRC
Attendance Register	Child's name and date of birth, Reasons for absence Child's arrival and departure time,	Legal obligation- Requirement of the statutory framework : EYFS and Childcare Register (Ofsted)	On Request with other agencies – eg. Ofsted, LSCB, LA or HMRC

Child Record and Emergency Contact	Information of child and emergency contact details from parents including family or friends	Legal obligation- Requirement of the statutory framework: EYFS Family and friends contact details covered by legal basis of 'consent'	The document may be shared with other agencies including Ofsted
Complaints Records	Child/family details, provider details	Legal obligation- Requirement of the statutory framework: EYFS and Childcare Register (Ofsted)	The document may be shared with other agencies including Ofsted

Concerns about a Child	Sensitive information on child or families, parents name and child's name	Legal obligation – requirement of the statutory framework EYFS	The document may be shared with other agencies including Ofsted
Childcare Contracts	Contract details between parent and provider. Sensitive details of child and families including parent and provider signatures	Insurance requirement and Legal obligation – requirement of the statutory framework of both EYFS and Childcare Register (Ofsted)	The document may be shared with other agencies including Ofsted and HMRC
Notification to terminate contract	Personal child and family details and signature and staff name	Legitimate interest as best practice to finalise contract. Contractual necessity of data retention.	This document may be shared with other agencies including Ofsted
Existing injuries record	Details of child's injuries from home or other setting includes personal details, parents and setting signatures and other setting details	Legitimate interests as required to support the child's health and safety	The document may be shared with other agencies including Ofsted
Illness Record	Child illness information, family and other setting details	Legitimate interest are required to support the child's health and safety	Document may be shared with other agencies including Ofsted
Incident Record	Personal child and family details, signatures of parent and setting	Legal obligation as required by the statutory framework of EYFS	Documents may be shared with other agencies including Ofsted
Informing Ofsted about changes / Ofsted notifications	Changes to Provider Details As required in the Compliance Handbook	Legal obligation as required by the statutory framework of the EYFS and Ofsted Requirements	Documents may be shared with other agencies including Ofsted

Learning and Development information	All About Me, Starting points, photos, videos, progress tracking, observations, assessments of learning and development e.g. two year old progress checks, termly reports (Hives), Support Plans and external professionals reports.	Legal obligation as required in statutory framework of EYFS and legitimate interest in Inspection Handbook as allow provider to track development effectively. Photo consent can be withdrawn at any time	May be shared with other agencies including Ofsted and other settings
Local Authority Funding form	Child and family personal information including NI details, two year and eypp codes and proof of DOB	Contractual obligation as required by LA for funding requirements	May be shared with other agencies included

Local Safeguarding Record Forms	CR 8 or CR 10 May have child or family personal information	Legal obligation as per EYFS and LSCP requirements	Documents may be shared with other agencies including ofsted and LSCP
Medication Administration record	Personal details of child, parents and setting signatures	Legal obligation required under statutory framework of EYFS	Document may be shared with other agencies including Ofsted
Permission forms	Child and parent names and signatures of parent and setting	Legal obligation under the EYFS statutory framework plus legitimate interests to provide high quality setting and photo permission can be withdrawn at any time	Document may be shared with other agencies including Ofsted
Physical Intervention record	Personal details about child and parent and setting signatures	Legal obligation as required by the statutory framework EYFS	Document may be shared with other agencies including Ofsted
Policies and procedures – acknowledgement of receipt	Parent confirmation that policies have been read and understood. Child details and parent and setting signatures	Legitimate interest and Legal obligation as required under the EYFS and Childcare Register (Ofsted)	Document may be shared with other agencies including ofsted
Visitor log	Date of visit, visitor name, reason for visit and times arriving and departing	Lawful basis to safeguard & protect children. Plus reasonably expect to provide high quality service and for fire safety/emergency purposes	Document may be shared with other agencies including ofsted

Individual rights

The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

Pre-Prep's responsibilities related to GDPR

As a school we understand we have responsibilities to ensure that we are following the GDPR legislation and procedures correctly. All our Rocket Pre-Preps have a designated Data Protection Controller: Miss Winsy, and all Office staff has also received relevant training and will therefore oversee how data is collected, stored and processed and will monitor access to it. Parents can contact Miss Winsy directly if they have any queries or complaints.
As we process personal individual data, all our Pre-Preps are registered with the Information Commissioner's Office (ICO) whose role is to uphold information rights in the public interest.
All staff understands and follows all of the Rocket Pre-Prep's policies and procedures which state the way we practice under the EYFS requirements and the level of conduct and that is expected of them, these policies are made available to parents via the school website at the Parents' Portal.
In case of a breach of personal data, the data protection controller, Miss Winsy, must be informed and an investigation must be immediately carried out.

Staff responsibilities in relation to GDPR

Staff are responsible for processing information correctly and being aware of what personal information can be shared and how to keep it secure.
Staff are aware of the Pre-Prep's procedures in relation to processing children's records, storing and taking photos on different devices, use of the Pre-Prep's social media platforms and the use of mobile devices for school purposes.

Use of computers and mobile devices Seesaw, school iPad's and laptops

Our Pre-Preps currently uses Seesaw as an online learning journal, which is hosted in the UK on secure servers complying with current GDPR, to observe, assess and track children's progress as well as securely sharing children's learning record with parents. Seesaw allows parents to have easier access at any time to their child's records and allows them to contribute to their child's Learning Journal by sharing their achievements at home.
As part of our commitment to safeguarding our children, all learning journeys are password protected so that only parents and carers can securely access the account of their child. Other than family, only the child's key person and the Head Teacher have access to the journal. If your child needs additional support, our Learning Support Coordinator will also have access to the learning journey in order to collaborate and track progress.

Each teacher has their own iPad (owned by the Pre-prep) to take the photographs, videos and notes while observing the children as part of our legal obligation under the EYFS Statutory Framework. These are then uploaded to the child's individual online journal to ensure children's progress, individual needs and learning and development is monitored.
Each staff member has a secure login which is password and pin protected. It is the responsibility of the staff to ensure that they do not leave themselves logged in to this platform whilst away from the device which they were using to access it. The passwords and usernames are not to be shared with anybody else. Photos and videos will be deleted ay the end of every day and IPads will be locked every night in a secure cupboard at the office. If they have permission to take the device they will adhere to all Policy requirements relating to e-safety, confidentiality and data protection, and safeguarding. No personal files or data that aren't for school use must be stored on school iPads or laptop devices.
All school devices such as laptops must be protected with up to date anti virus software to prevent information becoming vulnerable. Every member of staff has access to their own private cloud, OneDrive, which is hosted by Microsoft Business Education which complies with the new GDPR. Staff access their cloud, work email and any internal messaging such as Teams securely through our Microsoft account. Staff log-in and out every time they use any of these services.

If any member of staff suspects that their login details have been compromised in any way, they must inform the Head Teacher immediately and new login details will be created after ensuring no information has been compromised.

The Seesaw on-line Learning Journey system is hosted on secure dedicated servers based in the UK complying with the new GDPR. All data held on our Seesaw account is owned by each individual Pre-Prep so Chelsea Pre-Prep, Kingsland Pre-Prep and Grand West Pre-Prep. Each Rocket Pre-Prep is registered as controller of data with the Information Commissioner's Office (ICO) and is bound by the Data Protection Act and EYFS Statutory Framework requirements.

Rocket Pre-Preps email accounts

Each staff member has a designated school email which is used to contact the parents and carers of the children. This email address is only to be used for school correspondence and not for personal use. When sending group emails to more than one contact, staff ensure to use the BCC function on the email server to ensure that email addresses remain confidential. The email account is password protected and not to be left logged in. Staff access their work email securely through our Microsoft Business Education account.
Any sensitive data shared with external professionals (e.g. Local Authority) will be shared only with parental consent. All staff sending external data knows how to use Microsoft encryption to send data confidentially.
Individuals are accountable for their own use of the email system.

Concerning the use of ICT devices for school purposes, staff must not:

- Leave their school accounts logged in after using a device or whilst device is unattended.
- Use another staff member's user ID and login details to access private accounts.
- Access information that they are not authorised to.
- Leave their password unprotected.

- Connect personal devices to the Pre-Preps online systems.
- Use devices to download copyrighted materials illegally or for personal use.
- Download software without approval from the Head and management.
- Share unprotected sensitive personal data with anyone outside the school.
- Download explicit or inappropriate material with their device or any school device.
- Comment on the internet on the behalf of our Pre-Preps or Rocket Productions without prior approval.
- Use their device or email account to gamble online or access no school-related content.
- Use their email or messaging platform to make offensive and derogatory remarks.

Working from home or off site

Our Pre-Preps' staff have the option to take their school iPad's home to complete work in their own time if they need. Teachers must check first whether parents have given consent for their child's Seesaw learning journal to be updated outside school. Ofsted has stated that working on Seesaw does not constitute off-site storage in this context and allows staff to do so. We have the following guidelines to ensure the process of data is safe and secure:

- Pre-Prep devices must never be left unattended in public places
- All school devices must be password protected so only the key teacher can access it
- Software and programs used for work purposes such as Seesaw and Outlook must remain logged out, whilst the staff member is away from the device
- Only the staff member may use the device, it is not to be accessed by anybody else
- The Pre-Prep ICT equipment is strictly for work use only, not for personal use which would constitute gross misconduct
- Data must be protected from potential loss of the device (always store data through Seesaw or our Microsoft Business Education cloud. All data saved in the device must be deleted afterwards)

If a device is lost or stolen from a staff member, it must be reported to the data protection controller and the Head Teacher immediately. All steps must be taken to secure the data on the device if any. iPads will be deactivated remotely, laptops must be encrypted and password protected.

Viruses

All devices must be protected from potential cyber viruses. All laptops and desktops are secured with up to date antivirus software, this is not to be removed by staff members. This is managed by Abbey systems who check our systems annually and as needed.
If a virus is detected, the data protection controller must be informed and will remove the virus with the approved anti virus software.

Procedure in event of a staff member leaving

In event of a staff member leaving or in event of the contract being terminated, all of their work related data must be retained by the Pre-Prep. Once the staff member leaves they must not have access to any personal data associated with Chelsea Pre-Prep, Kingsland Pre-Prep, Grand West Pre-Prep, Rocket Productions, and any partner schools/business apart from their own personal documentation. Their account on our Pre-Prep software and any other access to platforms will be immediately removed. All staff are aware that they must not share any information or resources related to the Pre-Preps, Rocket Productions or any of the families/children/external professionals.

This document should be read alongside our Privacy Notice. Any queries please contact the office.