General Data Protection Regulation (GDPR) Policy

This policy covers the General Data Protection Regulations that come into force on 25th May 2018.

At Davidson-Roberts we are required to process relevant personal data as part of its operation and shall take all reasonable steps to do so in accordance with this policy and to comply with the privacy principles of the GDPR.

Article 5 of the GDPR requires that personal data shall be:

Lawfulness, Fairness and transparency- Personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals;

Purpose Limitation - Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;

Data minimisation - Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

Accuracy - Personal data shall be accurate and, where necessary, kept up to date; every reasonable step will 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;

Storage limitation- Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary 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;

Integrity and confidentiality - Personal data shall be 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."

Accountability - the controller shall be responsible for, and be able to demonstrate, compliance with the principles of the GDPR

We respect and comply with the individual rights of a person under the GDPR.

The GDPR provides the following rights for individuals:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing

General Data Protection Regulation (GDPR) Policy

6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

Processing may include obtaining, recording, holding, disposing, destroying or otherwise using data.

Any information which falls within the definition of personal data and is not otherwise exempt will remain

confidential and will only be disclosed to third parties with the consent of the appropriate individual or under the terms of this policy. The setting may from time to time be required to process sensitive personal data regarding a child in our care. We will share this data where there is a legal obligation to do so such as in a child protection investigation.

From May 25th 2018 we gain consent from all employees to hold personal information on them when they commence employment with us. Any employees working for the company prior to this date will be asked to give consent to hold the relevant data on them. All other information held on staff that is not needed will be disposed of in a safe and confidential way.

Data which may be held includes the following:

- List of names, addresses and home telephone numbers and emergency contact numbers of children attending and staff/ volunteers/ students whether on spreadsheet, paper or card indexes or the data base (Famly)
- Personal information about children as recorded on their registration forms and on the data base (Famly)
- Paper or computer based employee files containing employment records, bank account details and national insurance numbers, email addresses.
- Training records of staff
- Performance records of staff including supervision records, appraisals, file notes, capabilities procedures and disciplinary records
- Information contained on e-mail which may mention the individual's name
- Laptop computers holding personal data
- Children's assessment / observation records
- Information provided to, or received from, external sources/agencies
- Photographs- where consent has been granted.
- Incident and Accident reports
- Medication forms and Care plans
- Behavioural Plans
- Personal information of all staff, parents and children is also maintained on our Famly database and our Childcare online booking system. These are online, hosted service with a robust GDPR available at :
- Famly- please use the links at the bottom of the Famly website for terms and conditions and privacy/security notices.
- Childcare Online Booking System – privacy notice and agreement in place.
- Flick Learning (for staff only) – please use the links at the bottom of the flick learning site for terms and conditions and privacy notices.
- Perkbox (for staff only) – a copy of this agreement can be found on the Hub.

This list is not exhaustive and may be subject to change. Any information found not to be needed with be erased.

General Data Protection Regulation (GDPR) Policy

Sharing of information

Information and sharing is essential to meet the needs of the children and families who attend. Data may therefore be shared with and may be obtained from:

- Staff members /students /volunteers
- Schools
- Local settings as well as other settings within the company
- External agencies such as Local Safeguarding Children's Board, local Authority, Ofsted etc

Security of information

We will ensure that measures are taken to safeguard personal data. Each individual has a personal responsibility to ensure that any information of a personal or sensitive nature to which he/she has access in the course of his/ her work is protected from unauthorised access and disclosure and is kept confidential.

In particular, individuals must observe the following rules:

- Electronic storage of such material should be password protected, if there is any reason to believe that data security has been compromised, then passwords must be changed immediately. Contact Famly helpdesk for help if required
- Paper copies of personal data must be held in secure cabinets
- Information should be labelled as 'personal'
- Individuals must not disclose personal information except to authorised colleagues
- Particular care must be taken when exchanging information with third parties.
- Information must not be used for purposes other than that for which it was intended
- If records are needed to be taken off site (e.g. on laptops), appropriate security measures should be taken (e.g. laptops should never be left unattended in vehicles, and they should be stored securely off site) this has to be with permission from the manager. - see Handbook Policies
- All employees/ students/ volunteers must sign a confidentially agreement
- Where paper-based documents are removed from records these must be confidentially shredded.
- Personal data should not be retained for longer than necessary
- Memory sticks, discs etc will be only used by authorised people and will be stored securely when not in use.
- At any point a parent can make a request relating to their data. We will respond within 1 month of the request. We have the right to refuse a request if there is a lawful obligation to retain the data (from Ofsted or the EYFS) but we will inform the parents as to the reason what we cannot accept the request.

Disposal of information

Any data held on parents, children, staff or other employees that is not deemed necessary by law to retain will be shredded/burnt/deleted as appropriate.
All computers will be checked regularly to ensure any that all data that is not essential is removed, this includes the deletion of emails.
Annual 'housekeeping' will be undertaken to destroy any archived data that has reached the end of the retention period.

Data Breach

General Data Protection Regulation (GDPR) Policy

If we suspect there has been a breach of data we will contact the ICO (Information Commissioner's Office) within 72 hours of the incident.

How to contact the ICO
Call the breach reporting team: 0303 123 1113. They will also advise about data breach management.
Report online at ico.org.uk

What you need to tell them.

- What happened
- When it happened
- How it happened
- How many people could be affected?
- What sort of data has been breached?
- What did you have in place that could have stopped it?
- What have you done to help the people this affects?
- What have you learned?
- How can you stop similar breaches in the future?

What happens next?
The ICO may need to offer some guidance to help you out. Or they might need a bit more information, the ICO will contact you. Sometimes a more serious breach need more in-depth investigation.

We will keep an inventory record of any breaches of data.

Related Polices:
Confidentiality policy, Social Media and Networking Policy, Camera Policy, Computer and Information Technology Policy, Child protection and Safeguarding Policy

This policy was adopted by:	Date:
To be reviewed:	Signed:

Davidson-Roberts Ltd is registered with the ICO (Information Commissioner's Office)

Written in accordance with the *Statutory Framework for the Early Years Foundation Stage (2017): Safeguarding and Welfare Requirements: Information and Records [3.68-3.72]*