



Data Protection and GDPR Policy

Policy Statement

The Exwick Ark Ltd is committed to protecting the privacy, confidentiality, integrity and security of personal information relating to children, families, staff, volunteers, students, contractors and other individuals with whom we work.

This policy sets out how The Exwick Ark Ltd complies with the requirements of:

- The UK General Data Protection Regulation (UK GDPR)
- The Data Protection Act 2018
- The Human Rights Act 1998
- The Privacy and Electronic Communications Regulations (PECR)
- The Disclosure and Barring Service (DBS) Code of Practice
- All other relevant legislation relating to the collection, processing, retention and disposal of personal information.

This policy applies to all directors, managers, employees, volunteers, students, agency workers and contractors working on behalf of The Exwick Ark Ltd.

Roles and Responsibilities

The data controller is responsible for ensuring compliance with data protection legislation and overseeing the implementation of this policy. The designated Data Controller for The Exwick Ark Ltd is:

- Harriet Sharp
 - Telephone: 01392 425551
 - Email: harri@exwickark.co.uk

The deputy data controller for the Exwick Ark LTD is

- Joshua Stone
 - Telephone: 07512 962617
 - Email: josh@exwickark.co.uk

The Exwick Ark Ltd is registered with the Information Commissioner's Office (ICO). Further information regarding the ICO can be found here: [Information Commissioner's Office](#)

All staff, volunteers and contractors are responsible for handling personal information appropriately and completing any data protection and information security training required by the organisation.



Data Protection Principles

The Exwick Ark Ltd processes personal data in accordance with the principles set out in Article 5 of the UK GDPR.

Personal data must be:

- Processed lawfully, fairly and transparently.
- Collected for specified, explicit and legitimate purposes.
- Adequate, relevant and limited to what is necessary.
- Accurate and, where necessary, kept up to date.
- Retained only for as long as necessary.
- Processed securely using appropriate technical and organisational measures.
- Managed in a way that demonstrates accountability and compliance.

Lawful Basis for Processing

The Exwick Ark Ltd processes personal information under one or more lawful bases including:

- Compliance with a legal obligation.
- Performance of a contract.
- Protection of vital interests.
- Public task requirements.
- Legitimate interests.
- Consent, where consent is required.

Personal information will only be collected and processed where there is a clear and lawful purpose for doing so.

Collection and Use of Personal Data

The Exwick Ark Ltd collects personal information to:

- Deliver high-quality childcare and education.
- Support children's welfare, safeguarding and development.
- Manage staff employment, payroll and pension obligations.
- Meet legal and regulatory requirements.
- Administer government funding schemes.
- Support staff development and training.
- Operate the business effectively and safely.

Only information necessary for these purposes will be collected and retained.



Children's Records

Children's records are maintained to support learning, development, safeguarding and operational requirements.

Storage and Access

The primary system used for children's records is FAMLY. Within FAMLY, role-based permissions are applied to ensure that staff can only access the information necessary to carry out their duties.

Where information cannot be stored within FAMLY, it may be securely stored within:

- The Exwick Ark LTD's Microsoft 365 OneDrive
- The Exwick Ark LTD's Microsoft SharePoint (File store)
- Other approved systems authorised by the Data Controller

Access to children's information is restricted according to staff roles and responsibilities. Staff must only access information that is necessary for carrying out their duties.

Information relating to children should not be printed unless there is a legitimate operational, safeguarding, regulatory or legal requirement to do so. Where children's information is printed, it must:

- Be stored securely in an approved, lockable and non-portable filing cabinet or storage unit when not in use.
- Only be accessible to authorised members of staff.
- Not be removed from the setting unless authorised by the Data Controller or Designated Safeguarding Lead (DSL).
- Be disposed of securely through confidential shredding immediately after use or when no longer required.

Staff must take all reasonable precautions to prevent unauthorised access, loss, theft or disclosure of printed information containing personal data.

Information Sharing

Personal information relating to children may be shared with:

- Devon County Council
- Early Years Funding Teams
- Health professionals
- Schools and other educational providers
- Safeguarding agencies
- Other authorised agencies where there is a lawful basis to do so



Parental consent will be sought where appropriate unless sharing is required by law or safeguarding obligations.

Educational Records

Parents and carers may request access to their child's records by submitting a request to the Data Controller. Requests will normally be responded to within one calendar month and in accordance with UK GDPR requirements. Identity verification may be required before information is released.

Transition to Schools

Where a child moves to another setting or school, appropriate educational and developmental information may be transferred securely to support continuity of care and learning.

Staff Records

The Exwick Ark Ltd holds personal information about staff to:

- Assess suitability to work with children.
- Administer payroll and pensions.
- Meet HMRC obligations.
- Monitor qualifications and training.
- Support professional development.
- Meet health and safety obligations.
- Meet safeguarding and safer recruitment requirements.

Storage

Staff information may be stored within:

- Impact Early Years
- FAMILY
- Microsoft 365
- Secure physical personnel files

Access

Access is restricted to authorised personnel including:

- Company Directors
- Nursery Managers
- Data Controller
- Deputy Data Controller
- Approved payroll providers where required



Staff have access to their personal information through the Impact Early Years system. Staff are encouraged to regularly review their Impact Early Years profile to ensure that the information held about them is accurate, complete and up to date.

If a member of staff identifies any incorrect, incomplete or outdated information, they must notify their manager as soon as possible so that the records can be reviewed and updated where necessary.

DBS Information

As an organisation using the Disclosure and Barring Service (DBS) to assess suitability for positions of trust, The Exwick Ark Ltd complies fully with the DBS Code of Practice.

Storage and Access

The Exwick Ark Ltd will not routinely retain copies of DBS certificates.

The organisation will:

- Verify and record the DBS certificate number.
- Record the date of issue.
- Record the level of check obtained.
- Record recruitment decisions where appropriate.

Access to disclosure information is strictly limited to those entitled to see it as part of their duties. Any information relating to DBS checks is stored securely in Impact Early Years and access-controlled systems.

DBS Update Service

All staff are required to register with the DBS Update Service during induction where applicable. The Exwick Ark Ltd retains only the information necessary to perform status checks through the Update Service.

Retention

Where disclosure information is retained, it will not normally be kept for longer than six months following a recruitment decision unless exceptional circumstances apply.

Disposal

Disclosure information will be destroyed securely by:

- Shredding
- Pulping
- Secure electronic deletion

No unauthorised copies will be retained.

Data Sharing



The Exwick Ark Ltd only shares personal data where:

- There is a lawful basis to do so.
- Consent has been obtained where required.
- There is a safeguarding or legal requirement.
- The sharing is necessary to fulfil contractual obligations.

Third-party providers currently used may include:

- FAMLY
- Impact Early Years
- Activ8
- Devon County Council
- Payroll and pension providers
- Professional advisers and auditors

The organisation maintains appropriate Data Processing Agreements (DPAs), contractual arrangements or data sharing agreements with third-party providers where required by law.

At the point personal data is collected, individuals will be provided with a Privacy Notice which explains:

- The types of personal data being collected.
- The purposes for which the data will be used.
- The lawful basis for processing the data.
- Who the data may be shared with.
- How long the data will be retained.
- The individual's rights under UK GDPR.
- How to contact the Data Controller.
- How to raise concerns with the Information Commissioner's Office (ICO).

Privacy Notices are available on The Exwick Ark Ltd website and are provided at the point personal information is collected wherever practicable. This ensures that individuals are informed about how their personal information will be processed in accordance with the transparency requirements of the UK GDPR.

Information Security

The Exwick Ark Ltd implements appropriate technical and organisational measures to protect personal information. These measures include:

- Access Controls
- Role-based permissions.
- User account management.
- Regular reviews of access rights.



Authentication

- Microsoft Multi-Factor Authentication (MFA).
- Strong password requirements.
- Secure authentication controls on authorised systems.

Device Security

- Company-managed devices.
- BitLocker full disk encryption.
- Microsoft Defender security protections.
- Automatic and enforced software and security updates.

Cloud Security

Personal information is stored using approved cloud systems including:

- Microsoft 365
- FAMLY
- Impact Early Years

Monitoring

The Exwick Ark LTD works with Activ8 to manage:

- Device security
- Security monitoring
- User account administration
- Data protection controls

Personal Devices and Remote Working

Staff must not store children, parent or staff personal data on personal devices unless explicitly authorised by the Data Controller. Where authorisation is granted:

- Devices must be password protected.
- A separate work partition must be installed on the device through Activ8 and encryption must be enabled.
- MFA must be enabled where available.
- Information must only be stored for the minimum period necessary.

Where documents need to be downloaded:

- Files must be stored within Microsoft 365 OneDrive.
- Files must not be stored permanently on local devices.
- Any temporary files must be deleted when no longer required.
- Portable storage devices containing personal information must be Microsoft BitLocker encrypted.



All company-issued devices are centrally managed and protected through security controls implemented by The Exwick Ark Ltd and its IT provider Activ8. These controls include:

- Automatic saving and synchronisation of files to the user's Microsoft 365 OneDrive account by default.
- BitLocker full-disk encryption to protect data stored on the device.
- Remote device tracking and management capabilities.
- Remote data wipe functionality in the event a device is lost, stolen or compromised.
- Multi-Factor Authentication (MFA) for user access.
- Security monitoring, updates and endpoint protection managed through approved systems.

Staff must report any lost, stolen or compromised device immediately to their manager, the Data Controller, or Activ8 so that appropriate action can be taken to protect personal data.

Communications

The Exwick Ark Ltd will use FAMLY as its primary communication platform with parents wherever possible. Parents may use FAMLY to:

- Access information relating to their child.
- Update contact information.
- View reports and records.
- Receive communications from the nursery.

Where alternative communication methods are used, appropriate security measures will be applied. Parents have access too and are encouraged to ensure that the information we hold on them is up to date on FAMLY especially regarding communication preferences.

Staff must use authorised company systems when communicating about children, parents or staff.

Data Breaches

Any actual, suspected or potential personal data breach must be reported immediately to the Data Controller. Examples include:

- Information sent to the wrong recipient.
- Loss or theft of a device.
- Unauthorised access to records.
- Accidental disclosure of personal information.
- Malware, ransomware or cybersecurity incidents.



The Data Controller will:

- Assess the breach.
- Record the incident.
- Investigate the cause.
- Implement corrective actions.
- Notify the ICO where required.

Where a breach presents a risk to individuals' rights and freedoms, notification to the ICO will be made within 72 hours where legally required.

Retention and Disposal

Personal information will be retained in accordance with:

- Statutory requirements.
- Employment legislation.
- HMRC requirements.
- Safeguarding guidance.
- The Exwick Ark Ltd Data Retention Schedule.

When information is no longer required it will be securely destroyed through:

- Secure shredding.
- Confidential waste disposal.
- Secure electronic deletion.
- Removal from approved cloud systems.

Individual Rights

Individuals have the right to:

- Be informed about how their data is used.
- Access their personal information.
- Request rectification of inaccurate information.
- Request erasure where applicable.
- Restrict processing.
- Request data portability.
- Object to processing.
- Request review of automated decision making where applicable.

Requests should be submitted to the Data Controller. The Exwick Ark Ltd will normally respond within one calendar month.

Right to complain

Both staff and parents have the right to raise a data protection complaint directly with The Exwick Ark Ltd, as well as with the Information Commissioner's Office (ICO). Complaints may relate to, but are not limited to:

- How The Exwick Ark Ltd has handled a subject access request
- The security measures used to store personal information



- How personal information has been collected, used, or shared

Complaints can be made via email, in writing, or through other appropriate communication methods to the setting manager. All data protection complaints will be:

- Acknowledged within 30 days of receipt
- Investigated without undue delay
- Managed in a fair and transparent manner, with the complainant kept informed of progress
- Responded to with a clear outcome once the investigation is complete

Where a complaint involves access to personal data, The Exwick Ark Ltd may need to verify the identity of the individual. In such cases, a valid form of identification (e.g. passport or driving licence) may be requested before information is disclosed.

If you are dissatisfied with the outcome of your complaint, or wish to escalate the matter, you may contact the Information Commissioner's Office via [Make a complaint to the ICO](#).

Monitoring and Review

The Exwick Ark Ltd will carry out annual reviews of:

- Data protection practices.
- Information security measures.
- Data processing activities.
- Third-party providers.
- Risk assessments.

This policy will be reviewed annually or sooner where there are significant changes to legislation, regulatory requirements or organisational practices.