

Data Protection Policy

Policy Reference Number: G24

Effective Date:	September 2025	Review Date:	August 2030
P&P Review Group Approval Date:	August 2025	Board Approval Date:	September 2025
Owner:	Michaela Loughlin	Department:	Governance
Issued To:	<input checked="" type="checkbox"/> Board of Management <input checked="" type="checkbox"/> All Staff <input type="checkbox"/> ET/LT <input type="checkbox"/> Head Office Managers <input type="checkbox"/> C&S Managers <input type="checkbox"/> Department/Other: _____	Method of Delivery:	<input type="checkbox"/> Annual Declaration <input checked="" type="checkbox"/> LearnPro Individual Sign Off <input checked="" type="checkbox"/> Board Portal
Stakeholder Consultation	<input type="checkbox"/> All Staff <input checked="" type="checkbox"/> RGDP (DPO) <input type="checkbox"/> Union <input type="checkbox"/> Employee Voices Group <input type="checkbox"/> Head Office Managers <input type="checkbox"/> C&S Managers <input type="checkbox"/> Department/Other: _____	This policy will be reviewed every 5 years from the date of implementation or earlier if deemed appropriate for any legislation or regulatory changes. If this policy is not reviewed within the above timescale, the latest approved policy will continue to apply.	
Equality Impact Assessment		No	N/A

Version Control

Date	Owner	Version	Reason for Change
August 25	Head of Compliance & Improvement	4.0	Incorporates Data (Use and Access) Act 2025

Summary of Changes

Section	Change
1.1	Added Data (Use and Access) Act 2025
5.1	Elaborated on collection of personal data to reflect the Data (Use and Access Act 2025 - Personal data will only be used for the original purpose it was collected (whether from the data subject or otherwise) for specified, explicit and legitimate purposes and not further processed by or on behalf of the controller in a manner that is incompatible with the purposes for which the controller collected the data. For the avoidance of doubt, processing is not lawful by virtue only of it being processed in a manner that is compatible with the purposes for which the personal data was collected. If Ark wishes to use personal data for a different purpose, for example for research, the data subject will be notified prior to processing where required.
5.5	Added section on right to complaint
All	Information Commissioner's Office changed to Information Commission.

Contents

1.0	Policy Statement	4
1.1	Legal & Regulatory Framework.....	4
2.0	Scope.....	4
3.0	Roles & Responsibilities	5
4.0	Related Policies, Procedures & Documentation	5
	For organisations ICO	6
	GDPR Ark Housing	6
5.0	Data Protection	6
6.0	Training & Monitoring Requirements.....	10
6.1	Training	10
6.2	Monitoring	10

1.0 Policy Statement

Ark is committed to ensuring the lawful, fair and transparent management of personal data.

All Board of Management members and employees including temporary staff and volunteers have a responsibility to ensure compliance with this policy which sets out our commitment to process personal data in accordance with the relevant legislation.

Failure to comply with data protection legislation could lead to financial penalties, regulatory action, as well as reputational damage. Breaching this policy may result in disciplinary action, depending on the severity of the violation.

The purpose of this policy is to confirm our commitment to ensuring the secure and safe management of data held by us in relation to customers, staff and other individuals, and to set out our duties in processing and managing that data.

1.1 Legal & Regulatory Framework

It is a legal requirement that we process data correctly, and we will collect, handle and store personal information in accordance with the relevant legislation.

The relevant legislation in relation to the processing of data, which may be replaced or updated from time to time, is currently:

- UK General Data Protection Regulation;
- UK Data Protection Act 2018 (DPA 2018);
- Privacy and Electronic Communications Regulations 2003 (PECR);
- Data (Use and Access) Act 2025.

2.0 Scope

The Policy applies to all personal data that Ark holds relating to living identifiable individuals regardless of the category of data or the format of the data. Personal data is any data which could be used to identify a living individual including, e.g. name, address, email, postcode, CCTV image and photograph. Special Category personal data is any information relating to racial or ethnic origin, political opinions, religious beliefs, health (mental and physical), sexual orientation, Trades Union membership and criminal convictions.

The policy applies to personal data held or accessed on Ark premises or accessed remotely via home or mobile working. Personal data stored on personal and removable devices are also covered by this policy.

This policy, along with the associated Procedures, applies to all board of management members, employees and staff including temporary staff, agency staff and volunteers.

3.0 Roles & Responsibilities

There is a range of standard expectations which underpin all policies. Read more about standard [role and responsibilities](#) in addition, the following specific responsibilities apply to this policy.

All staff have a responsibility for ensuring personal data is collected, stored and handled appropriately and must ensure that it is handled and processed in compliance with data protection regulations, this policy and the data protection principles.

The Head of Compliance & Improvement and Ark's data protection lead, with advice and assistance from the Data Protection Officer (DPO), are responsible for monitoring compliance with this policy and the data protection legislation; managing personal data breaches and data subject rights; recording and maintaining appropriate records of processing activities and the documented evidence required for compliance.

4.0 Related Policies, Procedures & Documentation

G24a - Information Security Incident and Personal Data Breach Management Procedure;

G24b - Data Subject Rights Procedure;

G25d - Data Protection Impact Assessment Procedure;

G26e - CCTV procedure;

G24f - Smart doorbells procedure;

G25 - Records Management Policy;

G25a - Records Management Procedure.

[Ark's Vision, Mission & Values](#)

5.0 Data Protection

5.1 Compliance

Ark will comply with our legal obligations and the data protection principles by ensuring that personal data is:

- **Processed lawfully, fairly and in a transparent manner in relation to individuals.**

Individuals will be advised on the reasons for processing via a Privacy Notice. Where data subjects' consent is required to process personal data, consent will be requested in a manner that is clearly distinguishable from other matters, in an intelligible and easily accessible form, using clear and plain language. Data Subjects will be advised of their right to withdraw consent and the process for Data Subjects to withdraw consent will be simple.

- **Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.**

Personal data will only be used for the original purpose it was collected (whether from the data subject or otherwise) for specified, explicit and legitimate purposes and not further processed by or on behalf of the controller in a manner that is incompatible with the purposes for which the controller collected the data. For the avoidance of doubt, processing is not lawful by virtue only of it being processed in a manner that is compatible with the purposes for which the personal data was collected. If Ark wishes to use personal data for a different purpose, for example for research, the data subject will be notified prior to processing where required.

- **Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.**

Ark will only collect the minimum personal data required for the purpose. Any personal data deemed to be excessive or no longer required for the purposes collected for will be securely deleted. Any personal information that is optional for individuals to provide will be clearly marked as optional on any forms.

- **Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased or rectified without delay.**

Ark will take reasonable steps to keep personal data up to date, where relevant, to ensure accuracy. Any personal data found to be inaccurate will be updated promptly. Any inaccurate personal data that has been shared with third parties will also be updated.

- **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.**

Ark will hold data for the minimum time necessary to fulfil its purpose. Timescales for retention of personal data are outlined in our Retention Schedule (G25a). Data will be disposed of in a responsible manner ensuring confidentiality and security.

- **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.**

Ark will implement appropriate security measures to protect personal data. Personal data will only be accessible to those authorised to access personal data on a 'need to know' basis. Employees will keep data secure by taking sensible precautions and following the relevant Ark policies and procedures relating to data protection.

In addition, Ark will comply with the 'Accountability Principle' that states that organisations are to be responsible for, and be able to demonstrate, compliance with the above principles.

5.2 Data Sharing

In certain circumstances Ark may share personal data with third parties. This may be part of a regular exchange of data, one-off disclosures or in unexpected or emergency situations.

In all cases, appropriate security measures will be used when sharing any personal data.

Where data is shared regularly, a contract or data sharing agreement will be put in place to establish what data will be shared and the agreed purpose. Prior to sharing personal data, Ark will consider any legal implications of doing so.

Data Subjects will be advised of data sharing via the relevant Privacy Notice.

5.3 Data Processors

Where Ark engages Data Processors to process personal data on our behalf, we will ensure that:

- Data processors have appropriate organisational and technical security measures in place.
- No sub-processors are used without prior written consent from Ark.
- An appropriate contract or agreement is in place explaining the full requirements of the data processor.

5.4 Security Incident and Breach Management

Occasionally Ark may experience a data security incident or personal data breach; this could be if personal data is:

- Lost, e.g. misplacing documents or equipment that contain personal data through human error, via fire, flood or other damage to premises where data is stored.
- Stolen; theft or as a result of a targeted attack on our network (cyber-attack).
- Accidentally disclosed to an unauthorised individual, e.g. email or letter sent to the wrong address.
- Inappropriately accessed or used.

This list is provided to highlight examples and is not exhaustive.

All security incidents or personal data breaches will be reported to and managed by the data protection lead who will be advised and assisted by the DPO.

The Information Commission and the individuals affected will be notified promptly, if required.

All security incidents and personal data breaches will be managed in accordance with Ark's Information Security Incident and Personal Breach Management Procedure [G24a].

5.5 Individual Rights

Ark will uphold the rights of data subjects to access and retain control over their personal data in accordance with our Data Subject Rights Procedure [G24b]. Ark will comply with individuals':

- **Right to be Informed** – by ensuring individuals are informed of the reasons for processing their data in a clear, transparent and easily accessible form and informing them of all their rights.
- **Right to Access** – by ensuring that individuals are aware of their right to obtain confirmation that their data is being processed; access to copies of their personal data and other information such as a privacy notice and how to execute this right.

- **Right to Rectification** – by correcting personal data that is found to be inaccurate. We will advise data subjects on how to inform us that their data is inaccurate. Inaccuracies will be rectified without undue delay.
- **Right to Erasure** (sometimes referred to as ‘the right to be forgotten’) - we will advise data subjects of their right to request the deletion or removal of personal data where processing is no longer required or justified.
- **Rights to Restrict Processing** - we will restrict processing when a valid request is received by a data subject and inform individuals of how to exercise this right.
- **Right to Data Portability** – by allowing, where possible, data to be transferred to similar organisation in a machine-readable format.
- **Right to Object** – by stopping processing personal data, unless we can demonstrate legitimate grounds for the processing which override the interest, rights and freedoms of an individual, or the processing is for the establishment, exercise or defence of legal claims.
- **Right to complain** - Any breaches of GDPR will be dealt with in the first case by Ark. Data Protection Complaints should be sent to dataprotection@arkha.org.uk. If after that you are still unhappy with our handling of your GDPR issue, you still have the right to complain to the Information Commission.

5.6 Data Protection by Design

We have an obligation to implement technical and organisational measures to demonstrate that we have considered and integrated data protection into our processing activities.

When introducing any new type of processing, particularly using new technologies, we will take account of whether the processing is likely to result in a high risk to the rights and freedoms of individuals and consider the requirement for a Data Protection Impact Assessment (DPIA).

All new systems and policies including the processing of personal data will be reviewed by the policy owner or project lead to ensure compliance with the law and establish if a DPIA is required. As required, advice and assistance will be provided by the DPO and if it is confirmed that a DPIA is required, it will be carried out in accordance with Ark's DPIA Procedure [G24d].

6.0 Training & Monitoring Requirements

6.1 Training

Staff will be made aware of good practice in data protection and where to find guidance and support for data protection issues. They will have training appropriate to their needs and to the needs of the organisation as identified on their individual learning plans. Ark will ensure that all employees have an awareness of this policy and receive adequate training to enable them to effectively fulfil their roles and ensure personal data is stored and processed securely.

6.2 Monitoring

Regular monitoring and audits will be undertaken by the Head of Compliance & Improvement, Ark's data protection lead and/or DPO will regularly check compliance with the law, this policy and associated procedures.