Privacy and Data Protection Procedure

Procedure Reference:		G48	
Related Policy:		G24	
Effective date:	September 2019	**Review date:**	September 2021
Approved by SLT:		September 2019	
Owner:	John Rankin	**Job Title:**	Head of Q&C
To be issued to:		Board of Management ARK Management All Staff	
Method of Delivery:		LearnPro Classroom Training	

Version Control

Date	Owner	Version	Reason for Change
Sep 2019	**John Rankin**	**5.0**	**3 yearly review and review to add into new format**

Summary of Changes

Section	Change
Whole Procedure	**The previous version of the Privacy Policy, which was reviewed by the SLT in 2018, has now been reviewed to separate the policy and procedure elements into the new policy and procedure format. No substantive changes have been made to content.**

Privacy and Data Protection Procedure

Contents

1.0 Introduction

ARK Housing Association Ltd ('ARK') is committed to ensuring the secure and safe management of data held by us in relation to people who use our services, contractors, staff and other individuals. ARK's staff members have a responsibility to ensure compliance with the terms of this procedure, and to manage individuals' data in accordance with the systems and processes outlined in this procedure, and documentation referred to herein.

ARK needs to gather and use certain information about individuals. These can include people who use our services (tenants, people who use our Care and Support services, family members of people who use those services etc.), employees and other individuals that ARK has a relationship with. ARK manages a significant amount of data, from a variety of sources. This data contains Personal Data, Sensitive Personal Data (known as Special Category Personal Data under the General Data Protection Regulations or 'GDPR'), and in some circumstances Children's Personal Data.

This procedure sets out ARK's duties in processing that data, and the procedures for the management of such data.

This procedure should be read in conjunction with ARK's Privacy and Data Protection Policy (G24).

All employees are required to abide by this procedure, as well as ARK's Privacy and Data Protection Policy.

2.0 Data

ARK holds a variety of Data relating to individuals, including people who use our services, contractors and employees (also referred to as data subjects) which is known as Personal Data. The Personal Data held and processed by ARK is detailed within the Fair Processing Notices which are created, reviewed and updated regularly by our Data Protection Officer ('DPO').

2.1 Personal Data

'Personal Data' is that from which a living individual can be identified either by that data alone, or in conjunction with other data held by ARK.

2.2 Special Category Data

As well as Personal Data, ARK holds Personal data that is sensitive in nature (i.e. relates to or reveals a data subject's racial or ethnic origin, religious beliefs, political opinions, trade union membership, health or sexual orientation/ sex life, genetics). This is 'Special Category Personal Data' or 'Sensitive Personal Data'.

2.3 Children's Personal Data

In some circumstances, ARK also holds Personal Data related to children; where the data subjects are under 18 years of age.

3.0 Lawful Basis For Processing

3.1 Permitted Grounds for Processing

ARK is permitted to process Personal Data on behalf of data subjects provided it is doing so on one of the following grounds:

- Processing with the consent of the data subject (see clause 3.4 hereof);
- Processing is necessary for the performance of a contract between ARK and the data subject or for entering into a contract with the data subject;
- Processing is necessary for ARK's compliance with a legal obligation;
- Processing is necessary to protect the vital interests of the data subject or another person;
- Processing is necessary for the performance of a task carried out in the public interest or in the exercise of ARK's official authority; or
- Processing is necessary for the purposes of legitimate interests.

3.2 Fair Processing Notices

ARK's DPO has produced Fair Processing Notices (FPNs) which ARK is required to provide to all those whose Personal data is held by us. The relevant FPN must be provided to the data subject from the outset of processing their Personal Data and, where applicable, Special Category Personal Data or Sensitive Personal Data, and they should be advised of the terms of the FPN when it is provided to them.

It is the responsibility of staff in all relevant functions (eg Housing, Care and Support, Organisational Development) to ensure that the relevant FPN is provided to all data subjects at the outset of processing their data, and that a record is kept that the FPN has been provided. Guidance on this aspect can be obtained from ARK's DPO as necessary.

3.3 Employees

Employee Personal data and, where applicable, Special Category Personal Data or Sensitive Personal Data, is held and processed by ARK. Details of the data held and processing of that data is contained within the Employee FPN which is provided to Employees by the Organisational Development Team at the same time as their Contract of Employment.

A copy of any employee's Personal Data held by ARK is available upon written request by that employee, from the Head of People and Organisational Development.

3.4 Consent

Consent as a ground of processing may require to be used from time to time by ARK when processing Personal Data. It will be used only where no other alternative ground for processing is available. In the event that ARK requires to obtain consent to process a data subject's Personal Data, it shall obtain that consent in writing. The consent provided by the data subject must be freely given and the data subject will be required to sign a relevant consent form, if willing to consent. Any consent to be obtained by ARK must be for a specific and defined purpose (i.e. general consent cannot be sought).

3.5 Processing of Special Category Personal Data

In the event that ARK processes Special Category Personal Data or Sensitive Personal Data, we will do so in accordance with one of the following grounds of processing:

- The data subject has given explicit consent to the processing of this data for a specified purpose;
- Processing is necessary for carrying out obligations or exercising rights related to employment or social security;
- Processing is necessary to protect the vital interest of the data subject or, if the data subject is incapable of giving consent, the vital interests of another person;
- Processing is necessary for the establishment, exercise or defence of legal claims, or whenever court are acting in their judicial capacity;
- Processing is necessary for reasons of substantial public interest; or
- Processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.

4.0 Data Sharing

ARK shares its data with various third parties for numerous reasons in order that its day to day activities are carried out in accordance with relevant policies and procedures. In order that ARK can monitor compliance by these third parties with Data Protection laws, ARK will require the third party organisations to enter in to an Agreement with us governing the processing of data, security measures to be implemented and responsibility for breaches.

4.1 Data Sharing Agreements

Personal data is from time to time shared amongst ARK and third parties who require to process personal data that ARK processes as well. Both ARK and the third party will be processing that data in their individual capacities as data controllers.

Where ARK shares in the processing of personal data with a third party organisation (e.g. for processing of employees' pensions), we shall require the third party organisation to enter in to a Data Sharing Agreement with us in accordance with the terms of the model Data Sharing Agreement published by the Scottish Federation of Housing Associations in relevant guidance ('GDPR Model Documentation and Guidance Notes'), as adapted for our purposes by our DPO.

4.2 Data Processors

'Data processors' are third party entities that process personal data on behalf of ARK, and are engaged if certain aspects of our work are outsourced (e.g. repair works).

A data processor must comply with Data Protection laws. ARK's data processors must ensure that they have appropriate technical security measures in place, maintain records of processing activities and notify ARK if a data breach occurs.

If a data processor wishes to sub-contact their processing, our prior written consent must be obtained. Upon a sub-contracting of processing, the data processor will be liable in full for the data protection breaches of their sub-contractors.

Where ARK contracts with a third party to process personal data held by us, we shall require the third party to enter in to a Data Protection Addendum with us in accordance with the terms of the model Data Protection Addendum published in the Scottish Federation of Housing Association guidance ('GDPR Model Documentation and Guidance Notes'), as adapted for our purposes by our DPO.

If staff are unsure as to whether personal data can be shared with any third party or organisation, they should in the first instance seek guidance from their line manager, or from ARK's DPO.

5.0 Data Storage and Security

All employees are responsible for ensuring that all Personal Data relating to staff, tenants, people who use services, contractors etc which they hold and process, whether in electronic or paper format, is stored securely.

5.1 Paper Storage

If Personal Data is stored on paper it should be kept in a secure place where unauthorised personnel and third parties cannot access it, such as a locked drawer or locked filing cabinet. Employees should make sure that no Personal Data is left where unauthorised personnel or third parties can access it. When the Personal Data is no longer required it must be disposed of by the employee so as to ensure its destruction, in line with the requirements of this procedure, and other relevant guidance. If the Personal Data requires to be retained on

a physical file then the employee should ensure that it is affixed to the file which is then stored in accordance with ARK's storage provisions.

5.2 Electronic Storage

Personal Data stored electronically must also be protected from unauthorised use and access, in accordance with ARK's Computer System Security, Email and Internet Policy and Procedure (G15 and G46).

All employees and Board Members should ensure that:

- Electronic records are password protected. In ARK this is usually achieved through ensuring that data is only stored on ARK's secure server which can only be accessed through personal log-ins;
- Passwords are kept secure, changed regularly, and not shared with any unauthorised person;
- Computer screens are positioned away from windows to avoid accidental disclosure of personal information, and so that personal information is not visible to unauthorised staff;
- Computers are not left logged on and unattended;
- USB Sticks are only used as supplied by ARK's ICT team (such devices will always be encrypted);
- Where additional security is required, documents are password protected. To password protect a document go to 'Save As' and select 'Tools' on the 'Save As' toolbar. Then select 'Tools' and then 'General Options'. At the bottom of the Save Dialogue box type in your password. You will be asked to repeat your password; and
- When using the ARK General Drive, they consider the level of confidentiality of the relevant file, and ensure that it is saved in a location where it can only be accessed by authorised individuals- any queries in this regard can be directed to ARK's ICT Team.

5.3 Staff Responsibilities

All employees and Board Members should ensure that:

- personal information is not disclosed either orally or in writing to any unauthorised third party unless there are justified exceptional circumstances, such as assisting the Police with a criminal investigation, or assisting other emergency services;
- manual records containing personal information are not left unattended where they might be viewed by unauthorised staff or third parties;
- manual records and printouts no longer required are shredded and disposed of securely;
- particular care is taken if data is being removed from or transferred between ARK premises. All work must be kept confidential and, in the case of computerised information, every care should be taken to ensure that files are not exposed to the risk of virus infection;

- if the theft of personal information being removed from ARK premises would cause damage or distress if lost or stolen, that personal information must, if manual data, be stored securely at all times, and if electronic data, must be encrypted; and
- visitors to ARK premises should not be left unaccompanied in areas normally restricted to staff.

5.4 Email Security

All employees and Board Members should ensure that they always consider whether the content of emails should be encrypted or password protected. ARK's Head of ICT will be able to assist with advice and support on security if necessary.

All employees and Board Members should note and implement the following guidance as necessary:

- When you start to type in the name of the recipient, ARK's email software will suggest similar addresses that have been used before. If for example the person sending the email has previously emailed several people whose name or address starts the same way - eg "Fiona" - the auto-complete function may bring up several "Fionas". Staff should ensure that they choose the right address before they click 'send';
- To send an email to a recipient without revealing their address to other recipients, staff should make sure to use blind carbon copy (bcc), not carbon copy (cc). When you use cc every recipient of the message will be able to see the address it was sent to;
- Staff should be careful when using a group email address. Always check who is in the group and make sure you really want to send the message to everyone; and
- If an email is sent from a secure server to an insecure recipient, security will be threatened. Particular care should be taken when considering sending data to internet email accounts such as 'gmail', 'hotmail' or 'yahoo mail' You may need to check that the recipient's arrangements are secure enough before sending your message, and if in doubt please check with ARK's Head of ICT before sending,

Further guidance on the use of ARK's email system can be found in the Computer System Security, Email and Internet Policy G15.

5.5 Royal Mail/ Post Security

ARK is responsible for how we process all personal data that we hold, which includes data which we require to send by post. In that regard, all employees and Board Members should note and implement the following guidance as necessary:

- Always consider whether the data requires to be posted at all. Is there another more secure way of sharing the data, such as saving on a secure shared drive which is only accessible to relevant staff members, or sending via secure (eg password protected/ encrypted) email?
- If you do require to post personal data such as employee identification or information in relation to people who use services, either to another ARK office, or to an authorised third party, such as the Office for National Statistics, this should always be done via a secure, trackable postal system such as Royal Mail recorded delivery post; and
- Always take particular care to check all contents of the envelope are meant for the recipient, and check that the address you are posting data to is correct before posting. Keep the relevant receipt as a record of posting in case the letter does not arrive for any reason at its intended destination.

6.0 Breaches

A data breach can occur at any point when handling Personal Data and ARK has reporting duties in the event of a data breach or potential breach occurring. Breaches which pose a risk to the rights and freedoms of the data subjects who are subject of the breach require to be reported externally in accordance with Clause 6.2 hereof.

6.1 Internal Reporting

ARK takes the security of data very seriously and in the unlikely event of a breach will take the following steps:

- As soon as the breach or potential breach has occurred, and in any event no later than six (6) hours after it has occurred, the relevant staff member **must** notify the DPO in writing of (i) the breach; (ii) how it occurred; and (iii) what the likely impact of that breach is on any data subject(s);
- ARK must seek to contain the breach by whatever means available;
- The DPO will consider whether the breach is one which requires to be reported to the ICO and data subjects affected and do so in accordance with this clause 6;
- The DPO or relevant ARK employee will notify third parties in accordance with the terms of any applicable Data Sharing Agreements; and
- The DPO or relevant colleague/ function will put in place actions taken to mitigate any risk associated with the breach, for example via investigation of the breach, review of procedures in place, development of remedial actions.

6.2 Reporting to the ICO

The DPO will require to report any breaches which pose a risk to the rights and freedoms of the data subjects who are subject of the breach to the Information Commissioner's Office ("ICO") within 72 hours of the breach occurring. The DPO must also consider whether it is appropriate to notify those data subjects affected by the breach.

7.0 Data Protection Officer

A Data Protection Officer is an individual who has an over-arching responsibility and oversight over compliance by ARK with Data Protection laws. ARK has elected to appoint a Data Protection Officer whose details are noted on our website and contained within our Fair Processing Notices.

7.1 DPO Responsibilities

The DPO will be responsible for:

- monitoring ARK's compliance with Data Protection laws, ARK's Privacy and Data Protection Policy and this procedure (for example via the provision of training, audits, and advice);
- co-operating with and serving as ARK's contact for discussions with the ICO; and
- reporting breaches or suspected breaches to the ICO and data subjects in accordance with Clause 6 hereof.

8.0 Data Subject Rights

Certain rights are provided to data subjects under the GDPR. Data Subjects are entitled to view the personal data held about them by ARK, whether in written or electronic form.

Data subjects have a right to request a restriction of processing their data, a right to be forgotten and a right to object to ARK's processing of their data. These rights are notified to ARK's customers in our Fair Processing Notices.

8.1 Subject Access Requests

Data Subjects are permitted to view their data held by ARK, or by third parties such as contractors processing data on ARK's behalf, upon making a request to do so (a Subject Access Request). Upon receipt of a request by a data subject, ARK must respond to the Subject Access Request within one month of the date of receipt of the request. ARK:

- must provide the data subject with an electronic or hard copy of the personal data requested, unless any exemption to the provision of that data applies in law;
- where the personal data comprises data relating to other data subjects, must take reasonable steps to obtain consent from those data subjects to the disclosure of that personal data to the data subject who has made the Subject Access Request; or

- where ARK does not hold the personal data sought by the data subject, must confirm that it does not hold any personal data sought to the data subject as soon as practicably possible, and in any event, not later than one month from the date on which the request was made.

Subject Access Requests will only be refused, in accordance with the GDPR, in certain exceptional circumstances, whereby the request is either manifestly unfounded, excessive or if an exemption applies (e.g. the protection of the rights of others- where the information contains the personal data of more than one individual).

8.2 The Right to be Forgotten

A data subject can exercise their right to be forgotten by submitting a request in writing to ARK seeking that ARK erases the data subject's Personal Data in its entirety.

Each request received by ARK will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The DPO will have responsibility for accepting or refusing the data subject's request in accordance with this clause and will respond in writing to the request.

8.3 The Right to Restrict or Object to Processing

A data subject may request that ARK restricts its processing of the data subject's Personal Data, or object to the processing of that data.

In the event that any direct marketing is undertaken from time to time by ARK, a data subject has an absolute right to object to processing of this nature, and if we receive a written request to cease processing for this purpose, then we will do so immediately.

Each request received by ARK will require to be considered on its own merits and legal advice will require to be obtained in relation to such requests from time to time. The DPO will have responsibility for accepting or refusing the data subject's request in accordance with this clause and will respond in writing to the request.

9.0 Data Protection Impact Assessments ('DPIAs')

DPIAs are a means of assisting ARK to identify and reduce the risks that our operations have on personal privacy of data subjects.

9.1 When to Carry our a DPIA

ARK will:

- Carry out a DPIA before undertaking a project or processing activity which poses a "high risk" to an individual's privacy. High risk can include, but is not limited to, activities using information relating to health or race, or the implementation of a new IT system for storing and accessing Personal Data; and
- In carrying out a DPIA, include a description of the processing activity, its purpose, an assessment of the need for the processing, a summary of the risks identified and the measures that it will take to reduce those risks, and details of any security measures that require to be taken to protect the personal data.

9.2 Who Should Carry Out a DPIA

Any staff member who proposes carrying out a new project or processing activity which could involve a high risk to an individual's privacy should carry out a DPIA. ARK's DPO will be available to provide advice and support in relation to the decision whether to complete a DPIA, and the completion of the DPIA itself, as necessary.

9.3 DPIAs which Identify a High Risk Which Cannot be Reduced

ARK will require to consult the ICO in the event that a DPIA identifies a high level of risk which cannot be reduced. The DPO will be responsible for such reporting, and where a high level of risk is identified by those carrying out the DPIA they require to notify the DPO within five (5) working days.

10.0 Archiving, Retention and Destruction of Data

ARK cannot store and retain Personal Data indefinitely. It must ensure that Personal data is only retained for the period necessary. ARK will ensure that all Personal data is archived and destroyed in accordance with the periods specified in Data Retention Schedules for each function developed by relevant Heads of Service working alongside ARK's DPO, and staff should also consider whether any retention periods are in place in relevant agreements with third party organisations such as local authorities before destroying relevant data.

11.0 Employee and Board Member Responsibilities

This procedure applies to everyone in ARK and all staff, Board Members and relevant third parties have a responsibility to comply fully with its terms, the terms of ARK's Privacy and Data Protection Policy and the requirements of the GDPR and associated legislation. This includes ensuring that:

- they are familiar with ARK's Privacy and Data Protection Policy, this procedure, and any other associated policies and procedures; and
- the personal data they record is accurate and secure.

If employees or Board Members are unsure about anything relating to this procedure, the Privacy and Data Protection Policy, or data protection more generally, they should ask the DPO for advice as necessary.

Any breach of the Privacy and Data Protection Policy or Procedure may lead to disciplinary action being taken in accordance with ARK's Disciplinary Policy and Procedure (HR18). Further, the Information Commissioner's Office has warned that those who access or share personal data without a valid reason could face criminal prosecution.

12.0 Implementation and Review

12.1 Implementation

The Chief Executive is responsible for ensuring that this procedure is implemented.

Each Director and Manager is responsible for ensuring that this procedure is implemented by the staff for whom they are responsible.

In order to support with implementation, appropriate training and guidance will be developed and rolled out to relevant employees and Board Members.

Responsibility for monitoring the application of this procedure will rest with the Senior Leadership Team of ARK.

12.2 Review

The DPO, on behalf of the Chief Executive, will ensure that this procedure is reviewed regularly as necessary, and in any event not less than every three years.