

Ark Housing Association Ltd Privacy Notice for Employees

How we use your personal data

This privacy notice explains what information we collect, when we collect it and how we use this. During the course of our activities we will process personal data about you (which may be held on paper, electronically or otherwise), and we recognise the need to treat it in an appropriate and lawful manner. The purpose of this notice is to make you aware of how we will handle your information. This privacy notice is for employees, which sets out the information Ark holds about staff members, the purpose for which this data is held and the lawful basis on which it is held. Ark may process personal information without staff members' knowledge or consent, in accordance with this Notice, where this processing is required or permitted by law. Separate privacy notices are available for housing applicants, tenants, visitors to our website and premises, job applicants, contractors and suppliers, supported people and our management board members.

Who are we?

We are Ark Housing Association Ltd, a Scottish Charity (Scottish Charity Number SC015694), a registered society under the Co-operative and Community Benefit Societies Act 2014 with Registered Number 1899RS and having our registered office at The Priory, Canaan Lane, Edinburgh EH10 4SG.

Ark takes the issue of security and data protection very seriously and strictly adhere to guidelines published in the Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR), together with any domestic laws subsequently enacted. We are notified as a Data Controller with the Information Commissioner's Office under registration number Z9714372 and we are the data controller of any personal data that you provide to us.

Any questions relating to this notice and our privacy practices should be sent to either:

Our Head of Organisational Development michael.catlin@arkha.org.uk 0131 447 9027 The Priory, Canaan Lane, Edinburgh EH10 4SG

Our Data Protection Lead Officer dataprotection@arkha.org.uk, 0131 447 9027 The Priory, Canaan Lane, Edinburgh EH10 4SG

Our Data Protection Officer info@rgdp.co.uk 07741 738842 / 0131 222 3239 RGDP LLP Level 2, One Edinburgh Quay 133 Fountainbridge, Edinburgh EH3 9QG

Key Definitions

Data processing

Data processing is any activity that involves the use of personal data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring personal data to third parties.

Personal data

Personal data is any information identifying a data subject (a living person to whom the data relates). It includes information relating to a data subject that can be identified (directly or indirectly) from that data alone or in combination with other identifiers Ark possesses or can reasonably access. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Sensitive personal data

Sensitive personal data is a special category of information which relates to a data subject's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data. It also includes personal data relating to criminal offences and convictions.

How we collect information from you and what information we collect

The information we collect from you or from third parties may include:

- Name
- Date of Birth
- Address (over previous 10 years for purposes of disclosure referral)
- Employee Number
- Work location/ team
- Telephone Number
- E-mail address
- Bank details
- NI number
- Pension Number
- Salary information including payment of statutory sick pay and maternity, paternity, parental leave pay
- Relevant identification such as passport or driving licence
- Personal characteristics such as gender, trade union membership, health requirements, disability, religion, sexual orientation and ethnic group
- Criminal convictions
- Employment history
- Qualifications
- Nationality, and information in relation to restrictions to working in the UK
- Signature
- Absence information, and associated relevant health information
- Training records
- PVG Number
- Details of professional registrations such as SSSC registration and
- Emergency contact details.
- When your images and audio are captured on our CCTV systems

Fair Processing of Data

Data Protection principles

In processing staff members' data the following principles will be adhered to. Personal data will be:

- Used lawfully, fairly and in a transparent way;
- Collected only for valid purposes that are clearly explained and not used in any way that is incompatible with those purposes;
- Relevant to specific purposes and limited only to those purposes;
- Accurate and kept up to date;
- Kept only as long as necessary for the specified purposes; and
- Kept securely.

Lawful processing of personal data

Personal information will only be processed when there is a lawful basis for doing so. Most commonly, Ark will use personal information in the following circumstances:

- when it is needed to perform staff members' contracts of employment;
- when it is needed to comply with a legal obligation; or
- when it is necessary for Ark's legitimate interests (or those of a third party) and staff members' interests and fundamental rights do not override those interests.

We will use your information for:

- Administration of contracts of employment
- Payment of salaries
- Recruitment and selection
- Pensions and associated benefits
- Appraisal, training and development
- Membership of professional bodies
- The administration of formal processes such as grievance or disciplinary, and relevant business processes such as maintaining business continuity contacts lists
- Ensuring that we comply with relevant legal obligations, such as when we require to request a reference in relation to a prospective employee, or make a referral to a regulator such as the SSSC; and
- Ensuring that we comply with best practice guidance, and insurers' requirements, in relation to retention of records, in accordance with Ark's legitimate interests

Ark may also use personal information in the following situations, which are likely to be rare:

- when it is necessary to protect staff members' interests (or someone else's interests); or
- when it is necessary in the public interest [or for official purposes.

The lawful bases we may further rely on include:

- **Consent:** where you have given us clear consent for us to process your personal information for a specific purpose. This will only apply in limited circumstances where we have clearly asked for your consent;
- **Contract:** where our use of your personal information is necessary for a contract we have with you, or because you have asked us to take specific steps before entering into a contract. This includes where you apply for housing and in order to enter into and perform your tenancy agreement;
- **Legal obligation:** where our use of your personal information is necessary for us to comply with the law. This includes our regulatory obligations, such as those imposed on us by the Scottish Housing Regulator;
- **Vital interests:** where our use of your personal information is necessary to protect you or someone else's life;
- **Public task:** where our use of your personal information is necessary for us to perform a task in the public interest or for our official functions and the task or function has a clear basis in law. This may apply to our public functions as a registered social landlord; and
- **Legitimate interests:** where our use of your personal information is necessary for our legitimate interests or the legitimate interests of a third party (unless there is a good reason to protect your personal information which overrides our legitimate interests).

Lawful processing of sensitive personal data

Some of the personal data that we process in relation to you is called 'special category personal data'. This type of data is more sensitive and therefore needs more protection including an

additional legal basis. We process special category data, as relevant, in relation to gender, health and ethnic origin. We process this data so that we can carry out the obligations and exercise specific rights of the controller in the field of employment in so far as it is authorised by domestic law

We may also process special categories of personal information in the following circumstances:

- In limited circumstances, with explicit written consent;
- in order to meet legal obligations;
- when it is needed in the public interest, such as for equal opportunities monitoring [or
- when it is needed to assess working capacity on health grounds, subject to appropriate confidentiality safeguards.

Less commonly, Ark may process this type of information where it is needed in relation to legal claims or where it is needed to protect a staff member's interests (or someone else's interests) and the staff member is not capable of giving consent, or where a staff member has already made the information public. Ark may use particularly sensitive personal information in the following ways:

- information relating to leaves of absence, which may include sickness absence or family related leaves, may be used to comply with employment and other laws;
- information about staff members' physical or mental health, or disability status, may be used to ensure health and safety in the workplace and to assess fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits;
- information about race or national or ethnic origin, religious, philosophical or moral beliefs, or sexual life or sexual orientation, may be used to ensure meaningful equal opportunity monitoring and reporting; and
- information about trade union membership may be used to pay trade union premiums, register the status of a protected staff member and to comply with employment law obligations.

Lawful processing of information about criminal convictions

Ark envisages that it will hold information about criminal convictions. Ark will only use this information where it has a legal basis for processing the information. This will usually be where such processing is necessary to carry out Ark's obligations. Less commonly, Ark may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect a staff member's interests (or someone else's interests) and the staff member is not capable of giving consent, or where the staff member has already made the information public.

Ark will only collect information about criminal convictions if it is appropriate given the nature of the role and where it is legally able to do so. Where appropriate, Ark will collect information about criminal convictions as part of the recruitment process or may require staff members to disclose information about criminal convictions during the course of employment.

Consent to data processing

Ark does not require consent from staff members to process most types of staff member data. In addition, Ark will not usually need consent to use special categories of personal information in order to carry out legal obligations or exercise specific rights in the field of employment law. If a staff member fails to provide certain information when requested, Ark may not be able to perform the contract entered into with the staff member (such as paying the staff member or providing a benefit). Ark may also be prevented from complying with legal obligations (such as to ensure the health and safety of staff members).

In limited circumstances, for example, if a medical report is sought for the purposes of managing sickness absence, staff members may be asked for written consent to process sensitive data. In those circumstances, staff members will be provided with full details of the information that sought and the reason it is needed, so that staff members can carefully consider whether to consent. It is not a condition of staff members' contracts that staff members agree to any request for consent.

Where staff members have provided consent to the collection, processing and transfer of personal information for a specific purpose, they have the right to withdraw consent for that specific processing at any time. Once Ark has received notification of withdrawal of consent it will no longer process information for the purpose or purposes originally agreed to, unless it has another legitimate basis for doing so in law.

Automated decision making

Automated decision-making takes place when an electronic system uses personal information to make a decision without human intervention.

Ark may use automated decision-making in the following circumstances:

- Where staff members have been notified and given 21 days to request a reconsideration.
- Where it is necessary to perform a contract and appropriate measures are in place to safeguard staff members' rights.
- In limited circumstances, with staff members' explicit written consent and where appropriate measures are in place to safeguard staff member rights.

If Ark makes an automated decision on the basis of any particularly sensitive personal information, staff members will be asked for explicit written consent unless processing is justified in the public interest. Ark will put in place appropriate measures to safeguard staff member rights. Staff members will not be subject to decisions that will have a significant impact based solely on automated decision-making, unless Ark has a lawful basis for doing so and has given staff members prior notification.

Sharing of Your Information

The information you provide to us will be treated by us as confidential and will be processed only by our employees within the UK, subject to the comments in the 'Transfers outside the UK' section below. We may disclose your information to other third parties if we are required to by law or if they who act for us for the purposes set out in this notice or for other purposes approved by you, including the following:

- To support your recruitment with Ark, when we require to request a reference in relation to you, or with subsequent employers, when they ask us to provide a reference
- To process your regular salary payments
- To allow your pension provider to process pensions information and handle your pension
- To comply with the legal expectations of our regulators, such as the Care Inspectorate, Scottish Housing Regulator, SSSC, and Disclosure Scotland, as well as with the work of our auditors
- To manage your training and qualification records, where there is involvement by external funders, training providers, verifiers or accrediting agencies
- To deal with any issues which are raised in terms of our disciplinary or grievance policies, and also where these need to be reported to regulators, shared with ACAS, or shared with relevant legal or union representatives
- To provide an archive service for relevant former employee records; and
- If we enter into a joint venture with or are sold to or merged with another business entity, your information may be disclosed to our new business partners or owners.

Unless required to do so by law, we will not otherwise share, sell or distribute any of the information you provide to us without your consent.

Transfers outside the UK

When required, e.g., if we need to contact you or your representative outside the UK, we may transfer your information as follows:

- To EU/EEA countries or other countries which have an adequacy agreement with the UK.
- To countries outside the EU/EEA where there is no adequacy agreement. In these instances we will ensure that appropriate safeguards are in place and that personal information is treated by those third parties in a way that is consistent with and which respects the EU and UK laws on data protection: Further information about these protective measures can be requested from the contacts shown on page 1.

Security

When you give us information we take steps to make sure that your personal data is kept secure and safe. We will only store relevant information in accordance with our Data Protection policy and associated policies, copies of which are available on request.

How long we will keep your information

We review our data retention periods regularly and will only hold your personal data for as long as is necessary for the relevant activity, as required by law or as set out in any relevant contract we have with you. Our Retention procedure and schedule is available from our office on request.

Your Rights

Under certain circumstances, staff members have the right at any time to:

- Request access to personal information (commonly known as a “data subject access request”)
- To change incorrect or incomplete data
- Request erasure of personal information
- To object to processing of personal information where Ark is relying on a legitimate interest (or those of a third party) to lawfully process it
- Request the restriction of processing of personal information.
- Request the transfer of personal information to another party.

If you would like to exercise any of your rights, have any questions or would like to complain about the way that we process your personal data, please contact the Data Protection Lead at:

Ark Housing Association Ltd
The Priory
Canaan Lane
Edinburgh
EH10 4SG

Telephone: 0131 447 9027
Email: dataprotection@arkha.org.uk

Any requests received by us will be considered under applicable data protection legislation. Please note that, depending on the nature of the request, Ark may have good grounds for refusing to comply. If that is the case, the staff member will be given an explanation by Ark.

Data subject access requests

Staff members will not normally have to pay a fee to access personal information (or to exercise any of the other rights). However, Ark may charge a reasonable fee if the request for access is

clearly unfounded or excessive. Alternatively, Ark may refuse to comply with the request in such circumstances.

Ark may need to request specific information from the staff member to help confirm their identity and ensure the right to access the information (or to exercise any of the other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

COMPLIANCE WITH THIS POLICY

Ark's responsibility for compliance

Ark has appointed a Data Protection Lead who is tasked with overseeing compliance with this policy. If staff members have any questions about this policy or how Ark handles personal information, they should contact the Data Protection Lead. Staff members have the right to make a complaint at any time in relation to our use of your information to the Information Commissioner's Office (ICO).

The Information Commissioner's Office's contact details are below:

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

www.ico.org.uk

The accuracy of your information is important to us - please help us keep our records updated by informing us of any changes to your email address and other contact details.

Data security breaches

Ark has put in place procedures to deal with any data security breach and will notify staff members and any applicable regulator of a suspected breach where legally required to do so. Details of these measures are available upon request.

In certain circumstances, Ark will be required to notify regulators of a data security breach within 72 hours of the breach. Therefore, if a staff member becomes aware of a data security breach it is imperative that they report it to Data Protection Lead Officer immediately.

Privacy by design

Ark will have regard to the principles of this policy and relevant legislation when designing or implementing new systems or processes (known as "privacy by design").

Staff members' responsibility for compliance

All staff members, particularly those tasked with regularly handling personal data of colleagues or third parties, have responsibility for ensuring that processing meets the standards set out in this policy. Staff members should observe, as a minimum, the following rules:

- Staff members must observe to the letter any instruction or guidelines issued by Ark in relation to data protection.
- Staff members should not disclose personal data about Ark, colleague or third parties unless that disclosure is fair and lawful, in line with this policy;

- Staff members must take confidentiality and security seriously, whether the staff member considers the information to be sensitive or not.
- Any personal data collected or recorded manually which is to be inputted to an electronic system should be inputted accurately and without delay.
- Staff members must not make any oral or written reference to personal data held by Ark about any individual except to staff members of Ark who need the information for their work or an authorised recipient.
- Great care should be taken to establish the identity of any person asking for personal information and to make sure that the person is entitled to receive the information.
- If a staff member is asked by an unauthorised individual to provide details of personal information held by Ark the staff member should ask the individual to put their request in writing. If the request is in writing the staff member should pass it immediately to their line manager.
- Staff members must not use personal information for any purpose other than their work for Ark.
- If a staff member is in doubt about any matter to do with data protection they must refer the matter to their line manager immediately.
- Passwords should not be disclosed and should be changed regularly;
- Staff member or third party personal data should not be left unsecured or unattended, e.g. on public transport;
- Unauthorised use of computer equipment issued by Ark is not permitted;
- Staff members must follow Ark's "clear desk" policy and ensure that all confidential information, whether containing staff member or third party personal data or not, is secured when it is not in use or when the staff member is not at work;
- Staff members may use only encrypted Ark equipment to carry out work and must ensure that devices are password protected and locked when not in use. Staff members may use personal equipment to carry out work but must ensure that devices are password protected, locked when not in use and must not store any staff member or third party personal data locally on their device.
- Emails containing staff member or third party personal data must not be sent from a web-based email system;
- As far as possible, staff member or third party personal data contained in emails and attachments should be anonymised before it is sent by email; and
- Documents containing sensitive information should be password protected and, if the document requires to be transmitted, the document and password should be transmitted separately.

Any breach of the above rules will be taken seriously and, depending on the severity of the matter, may constitute gross misconduct which could lead to summary termination of employment.