PRIVACY POLICY

Contents

Effective from 25 May 2018
Reviewed - 9 December 2020 and 29 November 2023 (minor amendments on legal context and updated privacy notices)
Current To November 2028

1. Introduction

Ayrshire Housing (hereinafter the "association") is committed to ensuring the secure and safe management of data held by the association in relation to service users, staff and other individuals. The association's staff members have a responsibility to ensure compliance with the terms of this Policy, and to manage individuals' data in accordance with the procedures outlined in this policy and documentation referred to herein.

The association needs to gather and use certain information about individuals. These can include service users (applicants, tenants, factored owners etc.), employees and other individuals that the association has a relationship with. The association manages a significant amount of data, from a variety of sources. The data contains Personal Data and Sensitive Personal Data (known as Special Categories of Personal Data under the General Data Protection Regulation (UK GDPR).

This Policy sets out the association's duties in processing that data, and the purpose of this Policy is to set out the procedures for the management of such data.

2. Legislation

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

Ayrshire Housing takes data security very seriously. We adhere to the guidelines published in the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (UK GDPR) and the Data Protection Act 2018 (DPA 2018) together with any future legislation and regulations.

3. Data

3.1 The association holds a variety of data relating to individuals, including service users and employees (also referred to as data subjects) which is known as Personal Data. The Personal Data held and processed by the association is detailed within the Fair Processing Notice (published as the Privacy Notice) at Appendix 1.

3.1.1 "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 the association.

3.1.2 The association also 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, relates to health or sexual orientation). This is "Special Category Personal Data" or "Sensitive Personal Data".

4. Processing of Personal Data

4.1 The association 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 4.4 hereof);
- Processing is necessary for the performance of a contract between the association and the data subject or for entering into a contract with the data subject.
- Processing is necessary for the association'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 the association's official authority; or
- Processing is necessary for the purposes of legitimate interests.

4.2 Fair Processing Notice

4.2.1 The association has produced a Fair Processing Notice (published as the Privacy Notice) which it is required to provide to all service users whose Personal data is held by the association. The Notice must be provided to the user from the outset of processing their Personal Data and they should be advised of the terms of the Notice when it is provided to them.

4.2.2 The Privacy Notice at Appendix 1 sets out the Personal Data processed by the association and the basis for that processing. This document is provided to all the association's users at the outset of processing their data.

4.3 Employees

4.3.1 Employee personal data and, where applicable, Special Category Personal Data or Sensitive Personal Data, is held and processed by the association. Details of the data held and processing of that data is contained within a separate Employee Fair Processing Notice (Worker Privacy Notice – appendix 2) which is provided to employees at the same time as their Contract of Employment.

4.3.2 A copy of any employee's Personal Data held by the association is available upon written request by that employee from the association's Head of Performance & Quality.

4.4 Consent

Consent as a ground of processing may be used from time to time by the association when processing Personal Data. It may be used by the association where no other alternative ground for processing is available. In the event that the association 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 asked to sign a relevant consent form to confirm their consent. Any consent to be obtained by the association will be for a specific and defined purpose (i.e. general consent cannot be sought).

4.5 Processing of Special Category Personal Data or Sensitive Personal Data

In the event that the association processes Special Category Personal Data or Sensitive Personal Data, the association 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; and
- Processing is necessary for reasons of substantial public interest.

5. Data Sharing

5.1 The association shares its data with various third parties for many reasons so that its day-to-day activities can be carried out in accordance with the association's relevant policies and procedures. In order that the association can monitor compliance by these third parties with Data Protection laws, the association will require the third-party organisations to enter into an agreement with the association governing the processing of data, security measures and responsibility for breaches.

5.2 Data Sharing

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

5.2.2 Where the association shares in the processing of personal data with a third-party organisation (e.g. for processing of the employees' pension), it shall require the third-party organisation to enter into a Data Sharing Agreement with the association in accordance with the terms of the Model Data Sharing Agreement set out in Appendix 4 to this Policy.

5.3 Data Processors

Data processors are third party entities that process personal data on behalf of the association and are engaged if certain of the association's work is outsourced (e.g. payroll, maintenance and repair works).

5.3.1 A data processor must comply with Data Protection laws. The association's data processors must ensure they have appropriate technical security measures in place, maintain records of processing activities and notify the association if a data breach is suffered.

5.3.2 If a data processor wishes to sub-contact their processing, prior written consent of the association 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.

5.3.3 Where the association contracts with a third party to process personal data held by the association, it shall require the third party to enter into a Data Protection Addendum with the association in accordance with the terms of the Model Data Protection Addendum set out in Appendix 5 to this Policy.

6. Data Storage and Security

All Personal Data held by the association must be stored securely, whether electronically or in paper format.

6.1 Paper Storage

If Personal Data is stored on paper, it should be kept in a secure place where unauthorised personnel cannot access it. Employees should make sure that no Personal Data is left where unauthorised personnel can access it. When the Personal Data is no longer required it must be disposed of by the employee to ensure its destruction. If the Personal Data requires to be retained in a physical file, then the employee should ensure that it is affixed to the file which is then stored securely.

6.2 Electronic Storage

Personal Data stored electronically must also be protected from unauthorised use and access. Personal Data should be kept in a secure

communications environment when being sent internally or externally to the association's data processors or those with whom the association has entered into a Data Sharing Agreement. If Personal data is stored on removable media (eg CD, DVD, USB memory stick or portable hard drives) then that removable media must always be stored securely. Personal Data should not be saved directly to mobile devices without appropriate security settings. Details of CCTV image collection are contained in Appendix 3.

7. Breaches

7.1 A data breach can occur at any point when handling Personal Data and the association 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 7.3 hereof.

7.2 Internal Reporting

The association 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 hours after it has occurred, the Data Protection Officer (DPO) must be notified 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).
- The association will 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 Information Commissioner's Office (ICO) and the data subjects who were affected.
- The DPO will notify third parties in accordance with the terms of any applicable Data Sharing Agreements.

7.3 Reporting to the Information Commissioners Office (ICO)

The DPO will report any breaches which pose a risk to the rights and freedoms of the data subjects who are the subject of the breach to the ICO within seventy-two hours of the breach occurring. The DPO will also consider whether it is appropriate to notify those data subjects affected by the breach.

8. Data Protection Officer (DPO)

8.1. The DPO has an over-arching responsibility and oversight over compliance by the association with Data Protection laws. The association has elected to appoint a Data Protection Officer whose details are noted within the Fair Processing Notices.

8.2 The DPO is responsible for:

8.2.1 Monitoring the association's compliance with Data Protection laws and this Policy.
8.2.2 Co-operating with and serving as the association's contact for discussions with the ICO.
8.2.3 Reporting breaches or suspected breaches to the ICO and data subjects in accordance with Part 7 hereof.

9. Data Subject Rights

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

9.2 Data subjects have a right to request a restriction of processing their data, a right to be forgotten and a right to object to the association's processing of their data. These rights are notified to the association's tenants and other service users in the association's Fair Processing (Privacy) Notice.

9.3 Subject Access Requests

Data Subjects can request to view their data held by the association (a Subject Access Request). Upon receipt of a request by a Data Subject, the association will respond to the Subject Access Request within one month of the date of receipt of the request. The association:

9.3.1 Will 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.
9.3.2 Will 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 where the personal data comprises data relating to other data subjects; or
9.3.3 Will confirm 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 where they do not hold the personal data sought by the data subject.

9.4 The Right to be Forgotten

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

9.4.2 Each request received by the association will require to be considered on its own merits and legal advice may be needed in

relation to such requests from time to time. The DPO is responsible for accepting or refusing the data subject's request which will be done in writing.

9.5 The Right to Restrict or Object to Processing

9.5.1 A Data Subject may request that the association restrict its processing of the Data Subject's Personal Data, or object to the processing of that data.

If any direct marketing is undertaken from time to time by the association, a Data Subject has an absolute right to object to processing of this nature by the association, and if the association receives a written request to cease processing for this purpose, then it will do so immediately.

9.5.2 Each request received by the association 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 and will respond in writing to the request.

10. Privacy Impact Assessments (PIAs)

These are intended to identify and reduce the risks that our operations have on personal privacy of data subjects.

10.1 The association shall:

10.1.1 Carry out a PIA 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

10.1.2 In carrying out a PIA, 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.

10.3 The association will require to consult the ICO in the event that a PIA 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 PIA they must notify the DPO within five working days.

11. Archiving, Retention and Destruction of Data

The association will not store and retain Personal Data indefinitely. It undertakes that Personal Data is only retained for the period necessary. The association all ensure that all Personal Data is either securely archived or destroyed in accordance with the periods specified within the table at Appendix 6.

List of Appendices

1. Fair Processing Notice (published as the Privacy Notice)

2. Worker Privacy Notice

3. CCTV Policy

4. Model Data Sharing Agreement – to be used where it is appropriate for the association to take the lead in drafting such an agreement.

5. Model Data Protection Addendum

6. Data Retention Periods

APPENDIX ONE – GENERAL PRIVACY NOTICE (DECEMBER 2023)

How we use your personal information

This Privacy Notice explains what information we collect, when we collect it, and the reasons why we will hold and use your personal data, and your rights under current data protection law. In our dealings with you, we will handle personal data (which may be held on paper or electronically) about you. We recognise the need to treat it in an appropriate and lawful manner. We are committed to being transparent about how we collect and use your data, and to meeting our data protection obligations with you. This notice is to make you aware of how we will do this.

Ayrshire Housing takes data security very seriously. We adhere to the guidelines published in the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (UK GDPR) and the Data Protection Act 2018 (DPA 2018) together with any future legislation and regulations.

We are registered as a data controller under registration number **Z7777398** with the Information Commissioner's Office. This covers any personal data that you provide us with.

Data Protection Officer

We have appointed a Data Protection Officer. Our Data Protection Officer is the Head of Performance and Quality.

Any questions relating to this notice and our privacy practices should be sent to the Head of Performance and Quality at Ayrshire Housing, 119 Main Street, Ayr, KA8 8BX or info@ayrshirehousing.org.uk.

How we collect information from you and what information we collect

We collect information about you:

- When you apply for housing with us, become a tenant, request repairs and other services including medical adaptations, enter into a factoring agreement with ourselves or otherwise provide us with your personal details.
- When you apply to become a member of the association.
- When you apply to become a member of our Board (for more information on this, please see our Company Profile which is available on our website).
- From your use of our online services, for example to apply for or exchange housing, report any tenancy or factoring issue, make a complaint.
- From use of our website (www.ayrshirehousing.org.uk).
- From your arrangements to make payment to us.

- When you attend one of our events.
- From CCTV on our premises (for more information on this, please see our CCTV Policy which is available on our website).

What personal information do we collect?

We may collect the following information about you:

- Name.
- Address.
- Telephone number.
- E-mail address.
- National Insurance Number.
- Details of ethnicity, medical conditions and disability.
- Medical and other information as required by public health or health and safety guidance and policies.
- Next of kin.
- Details of previous experience, if you are applying to become a member of our Board (for more information on this please see our Company Profile which can be accessed through the 'About Us' page on our website).
- Payment information (such as bank details, payment card numbers, employment details, benefit entitlement and any other income and expenditure related information).
- Photographs and video footage of you for the association's promotional purposes including for use on the association's website or social media channels, as appropriate.
- Your IP address when accessing our website and online services.

We may receive the following information from third parties:

- Benefits information, including awards of Housing Benefit and Universal Credit.
- Payments made by you to us.
- Complaints or other communications regarding behaviour or other alleged breaches of the terms of your contract with us, including information obtained from Police Scotland.
- Reports as to the conduct or condition of your tenancy, including references from previous tenancies, and complaints of anti-social behaviour.

Attendance at Ayrshire Housing Events

At some events we run, there may be a photographer and/or videographer present and the images they provide may be used by us for the purposes of promoting the association's activities. This might include use in printed and online marketing, social media and press releases. If you would prefer us not to use your image, please contact the event organiser or speak to one of our staff on site at the event.

The data we hold on you will be stored securely in accordance with our Privacy Policy, which includes provision for retention periods.

Processing Special Category Personal Data

Special categories of information means information about your racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation, criminal convictions, offences or alleged offences, genetic data or biometric data for the purposes of uniquely identifying you.

We may collect and process special category personal data in the following circumstances:

- Where we need to carry out our legal obligations (such as required by public health) and in line with our Privacy Policy.
- Where is it needed in the public interest, such as equal opportunities monitoring, and in line with our Privacy Policy.
- Where it is necessary to enable us to perform our contract with you, such as where relevant adjustments are required.
- In limited circumstances, with your explicit written consent.

Why do we need this information about you and how it will be used?

We will process data in accordance with the following legal grounds:

Our Contract with You:

We need to process the data we hold on you in order that we comply with our obligations with you under the contract we have with each other.

These include:

- The need to process your data to provide you with the appropriate contract.
- To allow us to grant you a lease.
- To allow us to accept rent payments under the lease.
- To enable us to supply you with the services and information which you have requested in a safe manner.
- To enable us to respond to your repair request, housing application or complaint.
- To assess the information that we collect so that we can administer and improve the services we offer.
- To contact you to send you details of any changes to our services which may affect you; and
- For all other purposes consistent with the proper performance of our operations and business.

Legal Obligation:

We are required to process your data to comply with obligations to:

- Maintain accurate records, contact details, and emergency contact details; and
- Meet any regulatory and statutory requirements and checks in relation to your engagement with us.

Legitimate Interests:

We are also required to process your data in accordance with our legitimate interests, which can occur during and after our relationship with you, which will allow us to:

- Respond to and to defend legal claims in the event of a business sale or transfer.
- To contact you for your views on our services.
- To assess the use and function of our website.
- To provide our *HousingOnline* and *MyHome* services; and
- Use your photo on the association website if you are a Board member.

Sharing your information

The information you provide to us will be treated by us as confidential. We may disclose your information to other parties who act for us for the purposes set out in this notice or for purposes approved by you, including the following:

- If we enter into a joint venture with or merge with another organisation, your information may be disclosed to our new partners.
- If we are required to share our information with our professional advisors.
- To our suppliers and service providers to enable them to provide their services.
- If we instruct repair or maintenance works, your details may be disclosed to the contractor to allow the services to be provided in a safe manner to you and by our contractor.
- If we are investigating a complaint, information may be disclosed to Police Scotland, local authority departments, Scottish Fire & Rescue, our professional advisors and others involved in any complaint.
- If we are updating tenancy details, your information may be disclosed to third parties (such as utility companies and local authorities).
- If we are investigating payments made or otherwise, your information may be disclosed to payment processors, local authorities and the Department of Work & Pensions.
- If we are conducting a survey of our services, your information may be disclosed to third parties assisting in the compilation and analysis of the survey results.

Transfers outside the UK and European Economic Area

The information that you supply in connection with our *HousingOnline* housing application and mutual exchange services, and *My Home* tenancy service will only be stored and processed within the UK.

We may store your email address on e-newsletter services based outwith the UK or European Economic Area (EEA) solely for the purposes of communicating with you as part of your relationship with us. We will take reasonable steps to ensure that such services have UK GDPR compliant privacy policies in place.

Our consultants, contractors and suppliers as a condition of working with us may be required to communicate with us through online collaboration platforms which may be based outwith the EEA. We will take reasonable steps (such as contractual obligations with suppliers, etc) to ensure that such services have UK GDPR compliant privacy policies in place.

Security

When you give us information, we will ensure sure that your personal information is kept secure and safe. The safeguards that we have in place are described fully in our Privacy Policy a copy of which is available on our website.

Your Rights

You have the right at any time to:

- Be informed of the personal data we hold on you.
- Access and obtain a copy of all your personal data on request.
- Require us to correct any inaccuracies in your personal data.
- Require us to stop or restrict our processing concerning your personal data.
- Object to the processing of your personal data.
- Require us to delete what personal data of yours we hold.
- Personal data portability.
- Object to receiving any promotional communications from us.
- Be informed of automated decisions made in relation to you.
- Withdraw your consent to the processing of your personal data at any time, in instances where we are processing your personal data on your consent.

If you would like to exercise any of your rights above please contact us at info@ayrshirehousing.org.uk

You also have the right to complain to the Information Commissioner's Office in relation to our use of your information.

The Information Commissioner's contact details are:

The Information Commissioner's Office – Scotland
45 Melville Street, Edinburgh, EH3 7HL
Telephone: 0131 244 9001
Email: Scotland@ico.org.uk

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, or as required by law, or as set out in any relevant contract we have with you.

We will keep your information for no longer than the relevant period described in the data retention schedule attached to our Privacy Policy. A copy of which can be found on our website.

If you do not wish to provide your personal data

The provision of your personal data is a requirement necessary to enter into and perform your contract with us. Certain data, such as contact details, payment information, and identity information must be provided so that we can enter a contract with you. Failing to provide the data may mean that we are unable to perform our obligations under the contract.

Some personal data is required to fulfil our obligations under public health or health and safety guidance and policies. Failure to provide such data may mean failing to meet such obligations.

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.

APPENDIX TWO – WORKER PRIVACY NOTICE (DECEMBER 2023)

Worker Privacy Notice

Introduction

This notice explains what information we collect, when we collect it, the reasons why we will hold and use your personal data and your rights under the current data protection law. As your employer we will collect and process personal data relating to you to manage our contract with you. We recognise the need to treat it in an appropriate and lawful manner. We are committed to being transparent about how we collect and use your data, and to meeting our data protection obligations with you.

Ayrshire Housing takes data security very seriously. We adhere to the guidelines published in the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (UK GDPR) and the Data Protection Act 2018 (DPA 2018) together with any future legislation and regulations.

This notice does not form part of your contract of employment or engagement with us. It applies to all our employees, workers, apprentices and consultants, regardless of length of service, and may be amended at any time. If any amendments are made in the future, we will notify you.

Ayrshire Housing (the association) is registered as a data controller with the Information Commissioner's Office and our registered number is **Z7777398**.

Data Protection Officer

We have appointed a Data Protection Officer. This role is undertaken by the Head of Performance and Quality. Any questions relating to this notice and our privacy practices should be sent to the Head of Performance and Quality at Ayrshire Housing, 119 Main Street, Ayr, KA8 8BX or info@ayrshirehousing.org.uk.

How do we collect your personal information?

We may collect this information in several ways, which include:

- Recruitment processes including information obtained from agencies.
- Your identification documents you have given us.
- Background checks conditional for your engagement with us.
- PVG/Disclosure/DVLA checks relating to criminal convictions and offences.
- Former employers or other individuals whom you have given us permission to contact to provide us with a reference.
- Professional and training bodies connected with your employment.

- Web browsing history and email exchanges, but only if we have a reason to monitor this information.
- CCTV on our premises. For more information, please refer to our CCTV policy which can be found on our website.
- When you attend our events.

What personal information do we collect?

The association controls and processes a range of information about you. In this privacy notice 'your personal information' means your personal data i.e., information about you from which you can be identified. Your 'personal information' does not include data where your identity has been removed (anonymous data). It is important that your personal information that we hold, and process is accurate and up to date. Please keep us informed if your personal information changes during your engagement with us.
This data will include:

- Your name, address, and contact details including email address and telephone number, date of birth and sex.
- Appropriate health information from medical professionals, in order that we can manage any health-related situations that may have an impact on your ability to work with us.
- The terms and conditions of your employment or engagement with us.
- Details of your qualifications, skills, experience and work history, including start and end dates with previous employers and workplaces.
- Photographs and video footage of you for the association's promotional and operational purposes including for use on the association's website or social media channels, as appropriate.
- Membership of professional bodies.
- Membership of a trade union where you have consented to provide this information, e.g., through a mandate to pay your union dues from your salary or in furtherance of the recognition agreement.
- Information about your remuneration, including entitlement to benefits such as, pay, pension and holidays.
- Details of your bank account and national insurance number.
- Information about your marital status, next of kin, dependants and emergency contacts.
- Information about your nationality and entitlement to work in the UK.
- Information about any criminal convictions if relevant for your job.
- Details of your work pattern (days of work and working hours) and attendance at work.
- Details of periods of leave taken by you, including holiday, sickness absence, family leave and sabbaticals.
- Details of any disciplinary or grievance procedures in which you have been involved, including any warnings issued to you and related correspondence.

- Assessments of your performance, including personal development plans (PDPs), performance reviews and ratings, performance improvement plans and related correspondence.
- Information about medical or health conditions, including if you have a disability for which the association needs to make reasonable adjustments.
- Equal opportunities monitoring information about your ethnic origin, sexual orientation and religion or belief.
- Previous employment data. This data will include:
    - your work history with them, including the dates you were with them;
    - the work tasks you did;
    - your level of responsibility;
    - job title;
    - salary on leaving;
    - reason for leaving their workplace;
    - whether they would be happy to have you work for them again.
- CCTV footage of you on our premises

The data we hold on you will be stored securely in accordance with our Privacy Policy, which includes provision for retention periods.

Processing personal data

We will process data in accordance with the following legal grounds:

Our contract with you:

We need to process the data we hold on you in order that we comply with our obligations with you under the contract we have with each other.

These include:

- The need to process your data to provide you with an appropriate contract.
- To pay you in accordance with your employment contract.
- To administer your employment benefits.

Our legal obligations:

We are required to:

- Make checks regarding your right to work in the UK.
- Deduct tax, National Insurance, and administer your pension.
- Comply with health and safety laws.
- Enable you to take periods of leave to which you are entitled.

We are also required to process special categories of personal data, such as information about health or medical conditions to carry out our employment law obligations, such as those in relation to any disability you may have, or which arises.

Legitimate Interests:

We are also required to process your data in accordance with our legitimate interests, which can occur during and after our employment relationship, which will allow us to:

- Run recruitment and promotion processes.
- Use your photograph as required to ensure the effective delivery of services in accordance with the association's objectives, provide user assurance and to minimise potential fraud.
- Maintain accurate and up to date employment records, contact details, emergency contact details, and records of employee contractual and statutory rights.
- Operate and keep a record of disciplinary and grievance processes.
- Plan for career development, succession planning and workforce planning.
- Operate and keep a record for absence management to support workforce management and ensure that employees are receiving the pay or other benefits to which they are entitled.
- Obtain occupational health advice, to ensure that we comply with our duties in relation to individuals with disabilities, meet our obligations under health and safety law, and ensure that employees are receiving the pay or other benefits to which they are entitled.
- Operate and keep a record of other leave you may take including maternity, paternity, adoption, parental and shared parental leave, to allow effective workforce management, to ensure that the association complies with duties in relation to leave entitlement, and to ensure that employees are receiving the pay or other benefits to which they are entitled.
- Ensure effective general human resource and business administration.
- Provide references on request for current or past employees.
- Respond to and to defend legal claims in the event of a business sale or transfer.
- Any regulatory and statutory requirements and checks in relation to your engagement with us.
- Operate CCTV on our premises for security purposes.

Attendance at Association Events

At some events we run, there may be a photographer and/or videographer present and the images they provide may be used by us for the purposes of promoting the association's activities. This might include use of printed and online marketing, social media and press releases. If you would prefer us not to use your image, please contact the event organiser or speak to one of our staff on site at the event.

Processing Special Category Personal Data

Special categories of data means information about your racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation, criminal convictions, offences or alleged offences, genetic data or biometric data for the purposes of uniquely identifying you. There are specific legal reasons for processing this special data, details of these conditions are provided in the attached appendix.

We may require to process special category data in connection with:

- Equal opportunities information provided on appointment.
- Entitlement to work in the UK.
- Occupational health and absence management.
- Maintaining payments to a trade union and in connection with the operation of the recognition agreement between EVH and Unite the Union.

Employee Monitoring

We may require to carry out the following monitoring exercises in accordance with our procedures on security and appropriate usage:

- CCTV monitoring.
- Internet browsing and usage.
- Content and use of the work's email.
- Phone records both mobile and landline.
- Phone call recordings.

Sharing your information

The information you provide to us will be treated by us as confidential. We may disclose your information to other parties who act for us for the purposes set out in this notice or for purposes approved by you, including the following:

- If we enter into a joint venture with or merge with another organisation, your information may be disclosed to our new partners.
- If we contract a service provider who requires your personal information to perform those contracted services, your information may be disclosed.
- Where required, we will share information with professional advisors.
- If we enter into a contract to sell the association, your information may be disclosed to the buyer.

To process your data in accordance with the grounds stated above, we may share your information with:

Internally:

- Line managers.
- IT staff and consultants.
- HR staff.

Third parties:

- For the purposes of pre-employment checks; past employers, disclosure and PVG.
- For the purposes of processing data on behalf of us, e.g., payroll providers, advisors in relation to your contract of engagement and other associated policies and procedures, pension administrators and IT providers.
- Any other third parties as necessary to comply with your contract of engagement and our legal and statutory obligations with third party organisations.

Transfers outside the UK and European Economic Area

We may work with consultants, contractors or suppliers based outwith the UK or European Economic Area (EEA), during which relationship it may be necessary to provide them with your information for the grounds listed above. We will take reasonable steps (such as contractual obligations with suppliers, etc) to ensure that such services have UK GDPR compliant privacy procedures in place.

Our consultants, contractors and suppliers as a condition of working with us may be required to communicate with us through online collaboration platforms which may be based outwith the EEA. We will take reasonable steps (such as contractual obligations with suppliers, etc) to ensure that such services have UK GDPR compliant privacy procedures in place.

Security

When you give us information, we will ensure that it is kept secure and safe. The safeguards that we have in place are described fully in our Privacy Policy a copy of which is available on our website.

Your Rights

As a data subject, you have a number of rights:

- To be informed of the personal data we hold on you.
- To access and obtain a copy of all your personal data on request.
- Require the association to correct any inaccuracies in your personal data.
- Require the association to restrict the processing of your data.
- Require the association to stop or restrict our processing concerning your personal data and object to the processing of your personal data.

- To require us to delete the personal data we hold on you.
- To personal data portability.
- To be informed of automated decisions made in relation to you.
- In instances where we are processing your personal data on your consent, you may withdraw your consent to the processing.

If you would like to exercise any of the above rights, please contact the Data Protection Officer (see above).

You also have the right to complain to the Information Commissioner's Office in relation to our use of your information.

The Information Commissioner's contact details are:

The Information Commissioner's Office – Scotland
45 Melville Street, Edinburgh, EH3 7HL
Telephone: 0131 244 9001
Email: Scotland@ico.org.uk

Data Retention

We will only retain your personal information for as long as necessary to fulfil the purposes for which we collected it, including to satisfy any legal, accounting or reporting requirements.

We will retain all of your personal information during your engagement in accordance with the retention periods stated in our Privacy Policy after termination. This is to allow us to establish, exercise or defend legal claims, with the exception of the following:

- We will delete out-of-date contact, emergency contact, and bank account details whenever you provide us with updated details.
- We will retain current contact and bank account details during your engagement, and delete these when we have processed the final payment to you following the termination of your engagement.
- We will retain current emergency contact details during your engagement and delete these when your engagement ends.
- We will retain wage records, salary and benefits details, including pension and bonus details during your engagement and until the later of:

    - 6 years after termination; or
    - 6 years from the financial year-end in which payments were made.

- We will retain a copy of your driving licence, and MoT and driving insurance certificates during your engagement and delete these when your engagement ends.

If you do not wish to provide your personal data

You have obligations under your employment contract to provide the association with the necessary data. In particular, you are required to report absences from work and may be required to provide information about disciplinary or other matters under the implied duty of good faith. You may also have to provide us with data in order for you to exercise your statutory rights, such as in relation to statutory leave entitlements. Failing to provide the data may mean that you are unable to exercise your statutory rights.

Certain information, such as contact details, your right to work in the UK and payment details have to be provided so that we can enter into a contract of employment with you. If you do not provide the information, this will hinder our ability to administer the rights and obligations arising as a result of the employment relationship efficiently.

Automated Decision Making

Employment decisions are not based solely on automated decision making.

Acknowledgement of receiving and reading this worker privacy notice

I _____ [print name] confirm that I have read and understood the contents of this worker privacy notice.

Signed Date

Workers Privacy Notice, Appendix 1

Conditions for Processing Special Category Data

The information below is an extract from the ICO guidance and is available directly from their website: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

The conditions below are listed in Article 9(2)

(a) The data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) Processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation , association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) Processing relates to personal data which are manifestly made public by the data subject;

(f) Processing is necessary for the establishment, exercise of defence of legal claims or whenever courts are acting in their judicial capacity;

(g) Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment of the management of health or social care systems and services on the basis of Union or Member State law or

pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89 (1) based on Union Member State law which shall be proportionate to the aim pursued, respect the essence of the righto the data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Some of these conditions make reference to UK law, and the GDPR also gives member states the scope to add more conditions. The Data Protection Bill includes proposals for additional conditions and safeguards, and the ICO will publish more detailed guidance here once these provisions are finalised.

APPENDIX 3 – CCTV POLICY

Ayrshirehousing

Close Circuit Television at 119 Main Street, Ayr
Policy on its use

The association has installed Close Circuit Television (CCTV) in the following places:

- At the entrance, front and rear of our office.
- In the public and working areas of the office – this includes the reception and waiting area, public meeting rooms and interview rooms.

As expected by the Information Commissioner. We carried out a data protection impact assessment (DPIA) before commissioning the CCTV system. We have implemented a risk management strategy to ensure that it complies with our obligations under the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (UK GDPR) and the Data Protection Act 2018 (DPA 2018). The DPIA is available on our website and on request from our office.

The purpose of the CCTV is to:

- Protect users of the building including employees from criminal or anti-social behaviour.
- To minimise the risk of theft.
- To protect the premises when they are unoccupied.

To keep intrusion to minimum the following policy is applied:

- The recordings are of images only – there is no sound recording.
- All images are securely held and will only be observed by authorised employees.
- Unless required by the police or other legitimate individuals, images will be deleted after 30 days.

Further information:

Our reception staff will be delighted to answer any questions about the CCTV recording. Information is also available in advance of a visit to the office at www.ayrshirehousing.org.uk

You can find out about our approach to data protection in our Privacy Notice. The notice gives you details of your right to request copies of images and any other information we might hold on you. You can get a copy of the Privacy Notice at our reception or on our website.

Effective from 25 May 2018
Reviewed - 9 December 2020 and 29 November 2023 (minor amendments on legal context and updated privacy notices)
Current To November 2028

If you still have concerns, please ask to speak to our Data Protection Officer at 01292 880120 who will be pleased to answer your questions.

Ayrshirehousing

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

This template should be filled out at the start of any major project involving the use of personal data, or if you are making a significant change to an existing process. The final outcomes should be integrated into a project plan.

SUBMITTING DATA PROTECTION OFFICER DETAILS	
Name of Controller	Ayrshire Housing
Title of DPO	Head of Performance & Quality
Name of DPO	Caroline Donald

STEP 1: HOW DO WE DECIDE WHETHER TO DO A DPIA
Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you have identified the need for a DPIA.

As part of our office extension there is an intention to upgrade our CCTV system. This will include the introduction of external cameras to the front and rear of the building as well as cameras within the office in areas where staff are located and over-looking interview rooms where tenant/applicant interviews are being carried out. The CCTV system will not include sound.

The location of some of the cameras could result in systematic monitoring of employees' activities, including the monitoring of employees' workstations and internet activity.

This is a substantial change for the association and a DPIA is being undertaken to assess the extent to which monitoring is required, where it is required and at what times. We need to determine if the system is justifiable and that everyone who will be affected are consulted to assess the impact on their privacy and determine any safeguards which can and should be put in place.

We need to be mindful of the regulatory environment when using CCTV systems and consider our obligations under the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (UK GDPR) and the Data Protection Act 2018 (DPA 2018), Freedom of Information (Scotland) Act 2002, Human Rights Act 1998 (HRA) and CCTV Strategy for Scotland.

Using CCTV cameras can be privacy intrusive; they can place large numbers of law-abiding people under surveillance and recording their movements as they go about their day-to-day activities. We need to consider the problem(s) we are seeking to address; whether CCTV would be a justified and an effective solution or whether a better solution

exists and what affect it may have on individuals. We need to establish if we have a lawful basis for processing which is justified, necessary and proportionate.

We must establish who has responsibility for controlling the information we collect, i.e., deciding what is being recorded, how the information should be used and to whom it may be disclosed.

As the data controller we **would be** responsible for compliance with DPA and UK GDPR.

STEP 2: DESCRIBE THE PROCESSING

Describe the nature of your processing: how will you collect, use, store and delete the data? Will you be sharing data with anyone? Are they any types of processing involved which are likely to be considered as high risk?

How will we collect the data?

The data will be collected by cameras situated on our office at both the front and rear of the building with some cameras being located internally covering areas where staff are located or where tenants/applicants and other visitors are seated or being interviewed. The system will collect images only, not sound. The external cameras will point towards the ground to exclude filming any of the business premises on the opposite side of the road.

How will we use this data/equipment?

- The cameras will act as a deterrent against theft or other criminal activity.
- To provide employees and visitors with a safe environment to work and do business. By allowing us to monitor what is happening in the office we can help to protect staff and visitors against violence and protect them from false accusations.
- To monitor the office during periods when it is empty.
- In the event of a crime occurring, we can provide the Police with evidence.

How will we store the data?

The data will be stored on a CCTV 6 terabyte drive located in our server room. The data will not form part of our daily back-up programme.

Will the data be shared with anyone?

The data would be shared to the PCs of reception staff and others with dedicated responsibilities to monitor its use. It will also be loaded onto the mobile devices of staff on call if the intruder alarm is activated. We would anticipate that sharing of data would be controlled and consistent with the purpose for which the system was installed. For example, we would as a matter of course disclose information to the Police, but any other requests would be approached with care.

All staff are aware of the association's Privacy Policy and of the consequences of breaching it.

We would share information with members of the public should they make a legitimate subject access request. Clear guidance is in place through our Privacy Policy to determine who is authorised to make these disclosures and when it is appropriate to do so. A record of all disclosures will be kept.

We would ensure that viewing of live images is restricted to authorised persons unless the monitor displays a scene which is also in plain sight. Where possible, we would only view recorded images in a restricted area such as the server room or from under the counter of the reception desk.

Staff who are authorised to disclose data will be trained to use the system so that they are able to easily extract information in the prescribed format. We will ensure that, where required, 3rd party individuals' features are obscured to minimise the privacy intrusion.

We will ensure that any disclosures are made in a secure manner.

How would we delete the data?
DPA does not prescribe any specific minimum or maximum retention periods, but we would keep data for the shortest period necessary to serve our purpose. This will not be determined by the storage capacity of the drive.

The supplier proposes that the drive be over-written every 30 days. We will implement this proposal.

High Risk Processing
Under Article 35 of the GDPR we are required to carry out a DPIA for every processing operation which may result in "risks for the rights and freedoms of natural persons". Article 35(3) provides some examples of when a processing operation is likely to result in a high risk - condition [c] notes "a systematic monitoring of a publicly accessible area on a large scale".

In addition, CCTV monitoring does not always ensure that the data subject is aware of who is collecting their data and how it is being used. It may also be impossible for individuals to avoid being subject to such processing in publicly available spaces. The proposed location within the office of some of the cameras could also result in the monitoring of some employees' activities, including the monitoring of employees' workstations and internet activity. Under Article 35 of GDPR any excessive use of CCTV monitoring to profile employees is "high risk".

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals will be affected? What geographical areas does it cover?
What is the nature of the data, and does it include special category or criminal offence data?

CCTV, closed-circuit television also known as video surveillance. The data would not include special category or criminal offence data.

How much data will you be collecting and using?
Data will be continuously collected for 30 days. At the end of this period, it will be over-written. It is not possible to quantify how much data will be collected over that period. The data should **only** be used to respond to subject access requests and requests from the Police.

How often will it be collected?
24-hours per day.

How long will you keep it?
30 days.

How many individuals will be affected?
All employees of Ayrshire Housing and any visitors to the office. This will include service users such as tenants and applicants, contractors, Board members and other members of the public.

What geographical area does this cover?
119 Main Street, Ayr, KA8 8BX

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

Nature of Relationship, Control and Expectations

Staff Members [employed directly by Ayrshire Housing]
Under UK GDPR, employers are entitled to monitor employee activity if they have a lawful basis for doing so and the purpose of their monitoring is clearly communicated to employees in advance. Employees currently agree to this processing under the Workers Privacy Notice which everyone has signed. The notice states that employee monitoring may be required to carry out exercises in accordance with our "procedures on security and appropriate usage". These are described in the Conditions of Service, Code of Conduct and Staff Handbook

We cannot rely on consent as there is an imbalance of power in the employer/employee relationship. Employees can object to the use of CCTV cameras in a particular area which would then place the burden on Ayrshire Housing to demonstrate that we have "compelling legitimate grounds" for processing that override the employees' rights.

Members of the Public

CCTV monitoring does not always allow for the data subject to be aware of who is collecting their data and how it is being used. It may also be impossible for individuals to avoid being subject to such processing in publicly available spaces. Signage will be displayed prominently at the entrance so that individuals are aware of the CCTV installation and can ask for further information. Details of the installation will be included in the section on our office on our website

Due to the nature of the processing this could include children and other vulnerable groups. It is possible that children will be captured on CCTV, but the likelihood is that any children attending our office will be accompanied by an adult who will have the opportunity to review the CCTV information and the Privacy Notice to ensure that they are comfortable with our processing. It is also possible that vulnerable people could use our office, we will ensure that we provide all possible assistance to ensure that they understand the implications of our processing and the impact it might have on them.

Signage will be displayed at the public entrance and in the areas where CCTV cameras will be installed. This signage will be prominent.

Ayrshire Housing will consult with its IT specialists to ensure that appropriate safeguards are in place to mitigate any risks posed by data breach.

Technology in our area and current issues of public concern

We are not aware of any current areas of public concern regarding technology in our area, for example CCTV in public areas.

Approved Code of Conduct or Certification Scheme

We are not currently signed up to any certification scheme.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of processing – for you and more broadly?

Our purposes for processing are as stated above:

- The cameras will act as a deterrent against theft or criminal activity.
- To provide employees and visitors with a safe environment to work and do business. By allowing us to monitor what is happening in the office we can help to protect staff and visitors against violence and protect them from false accusations.
- To monitor the office during periods when it is empty.
- In the event of a crime occurring, we can provide the Police with evidence.

Data will **only** be used to review specific incidents that have occurred and will not be routinely used or checked.

The impact on individuals should be low, unless they have committed a crime at which point their data will be reported to the Police.

Step 3: Consultation Process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?
We will inform staff of the purpose of the installation. Notwithstanding the primary purpose to ensure a safe working environment, staff will be reminded that the installation does not extend the range of monitoring already permitted. It is not possible to consult with service users and the public in advance of the installation. We will however make information available so that they are given a degree of choice regarding their options in engaging with the association.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?
<u>Lawful Basis for Processing</u> Legitimate Interest • Prevention and detection of crime. • Safeguarding staff and visitors. • Ensuring compliance with health and safety procedures. <u>Does the processing achieve your purpose?</u> Yes, we can provide the police with enhanced information regarding any incidents that occur. CCTV will provide greater protection to individuals and improved health and safety. We are obligated to report crime and help the community at large to prevent crime or damage, this will allow us to achieve this purpose. <u>Is there another way to achieve the same outcome?</u> Not without using more intrusive methods such as a security guard posted outside the office. <u>How will you prevent function creep?</u> Function creep happens when we use technology and systems in ways beyond the original purpose, particularly when the new purpose results in invasion of privacy.

We will have a clear approach in place about our use of CCTV and we will not deviate from this. If we make any substantive modifications to the system, we will undertake a new DPIA.

How will you ensure data quality and data minimisation?

The data will be kept and used only to fulfil its original purpose. By working with our supplier, we will ensure that footage will continue to be of sufficient quality to aid easy identification of individuals. We will require the supplier to regularly update the software, especially in relation to security updates. We will ask that the drive is regularly checked to prevent degradation from constant over-writing. We will check the information provided by our supplier with our own IT Specialists.

We will ensure that recordings and logs are stored securely, and that access is limited to authorised persons only when required and the data is encrypted.

What information will you give individuals?

Clear signage will be posted wherever a camera is located informing individuals that CCTV is in operation. Further information will be readily available.

Employees have signed privacy notices providing them with information about monitoring.

We will ensure that individuals know how to make a subject access request, who it should be sent to and what information needs to be supplied with the request. We will inform individuals how to complain about the operation of our CCTV system or failure to comply with data protection legislation.

How will you support their rights?

Individuals have the right to request a copy of any CCTV footage in which they are clearly identifiable. If the request is valid and permissible, we will supply the individual with that footage within 30 days of the validation.

What measures do you take to ensure processors comply?

Staff will be trained in security procedures and will be advised about the potential consequences of misuse of the system.

Step 5: Identify and Assess Risk

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of Harm** [remote, possible or probable]	**Severity of Harm** [minimal, significant or severe]	**Overall Risk** [low, medium or high]
Policies not in place about CCTV and no nominated individual with responsibility.	Possible	Minimal	Medium
Staff not properly trained in how to handle information securely.	Possible	Minimal	Medium
Staff not properly trained in how to recognise a subject access request v FOISA	Probable	Significant	Medium
Staff who are authorised to access the cameras not familiar with the system, and with the processes for reviewing footage and extracting it if required.	Possible	Minimal	Medium
Staff not trained on how to handle a request for information from the Police.	Probable	Significant	Medium
Data breach, safeguards not in place to protect the data and ensure it is stored securely.	Probable	Significant	Medium
Data breach, information is disclosed but not delivered safely to the intended recipient.	Possible	Minimal	Medium
Access to data not restricted.	Possible	Significant	Medium
Staff misuse data.	Possible	Significant	Low
Data deletion not effective or being adhered to. Retention Policy not in place or adequate. Information not being permanently deleted.	Possible	Minimum	Medium
Image quality poor and not fit for purpose.	Remote	Minimal	Low
Are there security safeguards in place to prohibit interception and unauthorised access?	Remote	Minimal	Low
Have we notified individuals using privacy notices (where applicable)	Remote	Minimal	Low
Is the correct signage in place?	Remote	Minimal	Low
Are the cameras correctly placed? Will they work after dark? Are cable elements adequately protected from the elements? In workplace, consider the expectation of privacy (i.e., in social areas).	Remote	Minimal	Low
Do we have a maintenance contract to ensure our equipment is properly maintained and up to date (security software)?	Remote	Minimal	Low
Regular review of whether CCTV is still the best solution not undertaken.	Remote	Minimal	Low

Staff invasion of privacy challenge due to positioning of cameras.	Possible	Minimal	Medium

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5.				
Risk	**Options to reduce or eliminate risk** In addition to the existing policies in place regarding privacy, data management and staff conduct, the identified risks will be addressed by applying the measures described above at steps 2 to 4.	**Effect on Risk** [Eliminated, reduced, accepted] Reduced to an acceptable level.	**Residual Risk** [Low, medium, high] Low	**Measure Approved** [Yes/No] Yes

Step 7: Sign off and record outcomes

Item	Name/Position/Date	Notes
Measure approved by:	Alan Park, DPO, 26 April 2021	Implementation of measures checked after first month of operation.
Residual Risks approved by:	Deemed low and approved by Jim Whiston, Director, 26 April 2021.	If accepting any residual high risks, consult ICO before going ahead.
DPO Advice provided:	Agreed that processing can proceed.	DPO should advise on compliance. Step 6 measures and whether processing can proceed.
Summary of DPO Advice: Full implementation of the measures identified above required.		
DPO Advice accepted or overruled by:	Accepted by Jim Whiston Director, 26 April 2021	If overruled, you must explain the reason why.
Comments: none.		
Consultation responses reviewed by:	Not applicable, see step 3.	If your decision departs from individuals views, you must explain your reasons.
Comments: none.		

This DPIA will be kept under review by:	Caroline Donald, DPO	The DPO should also review ongoing compliance with DPIA.

APPENDIX 4 – MODEL DATA SHARING AGREEMENT

MODEL DATA SHARING AGREEMENT

between

Ayrshire Housing, a Scottish Charity (Scottish Charity Number SC027906), registered in terms of the Companies Acts with registered number (185652) and having its registered office/main office at 119 Main Street, AYR, KA8 8BX ("the association);

And

#[Insert organisation name, a # [e.g. Company] registered in terms of the Companies Acts with registered number [registered number] and having its registered office/main office at #[address]] ("#[Party 2]")]") [Drafting note: amend from Party 2 to suitable defined term];

(each a "Party" and together the "Parties").

WHEREAS

Drafting Note: Further detail will require to be inserted here to confirm relationship between Parties to the Agreement. This will depend on the precise nature of relationship so will require to be adapted for every individual use of this model Agreement.

(a) The association and [*Insert name of party*] ("[Party 2]") intend that this data sharing agreement will form the basis of the data sharing arrangements between the parties (the "Agreement"); and

(b) The intention of the Parties is that they shall each be independent Data Controllers in respect of the Data that they process under this Agreement.

(c) Nothing in this Agreement shall alter, supersede, or in any other way affect the terms of #[***insert details of relationship/ contract with Party 2***]

NOW THEREFORE IT IS AGREED AS FOLLOWS:

1 DEFINITIONS

1.1 In construing this Agreement, capitalised words and expressions shall have the meaning set out opposite:

"Agreement" means this Data Sharing Agreement, as amended from time to time in accordance with its terms, including the Schedule;

"Business Day" means any day which is not a Saturday, a Sunday or a bank or public holiday throughout Scotland;

"Data" means the information which contains Personal Data and Sensitive Personal Data (both of which have the definition ascribed to them in Data Protection Law) described in Part 1;

"Data Controller" has the meaning set out in Data Protection Law;

"Disclosing Party" means the Party (being either the Association or #[Party 2], as appropriate) disclosing Data (or on behalf of whom Data is disclosed to the Data Recipient);

"Data Protection Law" means Law relating to data protection, the processing of personal data and privacy from time to time, including:

(a) the Data Protection Act 2018;
(b) the UK GDPR ("GDPR"); and
(c) any legislation that, in respect of the United Kingdom, replaces, or enacts into United Kingdom domestic law, the proposed Regulation on Privacy and Electronic Communications or any other law relating to data protection, the processing of personal data and privacy as a consequence of the United Kingdom leaving the European Union;

"Data Recipient" means the party (being either the Association or #[Party 2], as appropriate) to whom Data is disclosed;
"Data Subject" means any identifiable individual to whom any Data relates: and the categories of data subjects within the scope of this Agreement are listed in Part 1;
"Data Subject Request" means a written request of either party as Data Controller by or on behalf of a Data Subject to exercise any rights conferred by Data Protection Law in relation to the data or the activities of the parties contemplated by this Agreement;
"Disclosing Party" means the party (being either the Association or #[Party 2], as appropriate) disclosing Data to the Data Recipient;
"Information Commissioner" means the UK Information Commissioner and any successor;
"Law" means any statute, directive, other legislation, law or regulation in whatever form, delegated act (under any of the foregoing), rule, order of any court having valid jurisdiction or other binding restriction, decision or guidance in force from time to time;
"Legal Basis" means in relation to either Party, the legal basis for sharing the Data as described in Clause **Error! Reference source not found.** and as set out in Part 2;
"Purpose" means the purpose referred to in Part 2;
"Representatives" means, as the context requires, the representative of the Association and/or the representative of #[Party 2] as detailed in Part 4 of the Schedule. The same may be changed from time to time on notice in writing by the relevant Party to the other Party;
"Schedule" means the Schedule in 6 Parts annexed to this Agreement and a reference to a "Part" is to a Part of the Schedule; and
"Security Measures" has the meaning given to that term in Clause **Error! Reference source not found.**.

1.2 In this Agreement unless the context otherwise requires:

1.2.1 words and expressions defined in Data Protection Law shall have the same meanings in this Agreement so that, in the case of Data Protection Law, words and expressions shall be interpreted in accordance with:
(a) the Data Protection Act 1998, in respect of processing undertaken on or before 24 May 2018;
(b) the UK General Data Protection Regulation, in respect of processing undertaken on or after 25 May 2018; and
(c) in respect of processing undertaken on or after the date on which legislation comes into force that replaces, or enacts into United

Kingdom domestic law, the UK General Data Protection Regulation, that legislation;

1.2.2 more generally, references to statutory provisions include those statutory provisions as amended, replaced, re-enacted for the time being in force and shall include any bye-laws, statutory instruments, rules, regulations, orders, notices, codes of practice, directions, consents or permissions and guidelines (together with any conditions attached to the foregoing) made thereunder;

DATA SHARING

Purpose and Legal Basis

1.3 The Parties agree to share the Data for the Purpose in accordance with the provisions of Part 2 of the Schedule.

1.4 Save as provided for in this Agreement, the Parties agree not to use any Data disclosed in terms of this Agreement in a way that is incompatible with the Purpose.

1.5 Each Party shall ensure that it processes the Data fairly and lawfully in accordance with Data Protection Law and each Party as Disclosing Party warrants to the other Party in relation to any Data disclosed, that such disclosure is justified by a Legal Basis.

Parties Relationship

1.6 The Parties agree that the relationship between them is such that any processing of the Data shall be on a Data Controller to Data Controller basis. The Data Recipient agrees that:

1.6.1 it is a separate and independent Data Controller in respect of the Data that it processes under this Agreement, and that the Parties are separately and individually responsible for compliance with Data Protection Law;

1.6.2 it is responsible for complying with the obligations incumbent on it as a Data Controller under Data Protection Law (including responding to any Data Subject Request);

1.6.3 it shall comply with its obligations under Part 6 of the Schedule;

1.6.4 it shall not transfer any of the Data outside the United Kingdom except to the extent agreed by the Disclosing Party;

1.6.5 Provided that where the Data has been transferred outside the United Kingdom, the Disclosing Party may require that the Data is transferred back to within the United Kingdom:

(a) on giving not less than 3 months' notice in writing to that effect; or

(b) at any time in the event of a change in Law which makes it unlawful for the Data to be processed in the jurisdiction outside the United Kingdom where it is being processed; and

1.6.6 it shall implement appropriate technical and organisational measures including the security measures set out in Part 5 of the Schedule (the "**Security Measures**"), so as to ensure an appropriate level of security is adopted to mitigate the risks associated with its processing of the Data, including against unauthorised or unlawful processing, accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or damage or access to such Data.

1.7 The Disclosing Party undertakes to notify in writing the other as soon as practicable if an error is discovered in Data which has been provided to the Data Recipient, to ensure that the Data Recipient is then able to correct its records. This will happen whether the error is discovered through existing Data quality initiatives or is flagged up through some other route (such as the existence of errors being directly notified to the Disclosing Party by the Data Subjects themselves).

Transferring Data

1.8 Subject to the Data Recipient's compliance with the terms of this Agreement, the Disclosing Party undertakes to endeavour to provide the Data to the Data Recipient on a non-exclusive basis in accordance with the transfer arrangements detailed in Part 3 of the Schedule.

2 BREACH NOTIFICATION

2.1 Each Party shall, promptly (and, in any event, no later than 12 hours after becoming aware of the breach or suspected breach) notify the other party in writing of any breach or suspected breach of any of that Party's obligations in terms of Clauses 1 and/or 2 and of any other unauthorised or unlawful processing of any of the Data and any other loss or destruction of or damage to any of the Data. Such notification shall specify (at a minimum):

2.1.1 the nature of the personal data breach or suspected breach;
2.1.2 the date and time of occurrence;
2.1.3 the extent of the Data and Data Subjects affected or potentially affected, the likely consequences of any breach (in the case of a suspected breach, should it have occurred) for Data Subjects affected by it and any measures taken or proposed to be taken by the that party to contain the breach or suspected breach; and
2.1.4 any other information that the other Party shall require in order to discharge its responsibilities under Data Protection Law in relation to such breach or suspected breach.

2.2 The Party who has suffered the breach or suspected breach shall thereafter promptly, at the other Party's expense (i) provide the other Party with all such

information as the other Party reasonably requests in connection with such breach or suspected breach; (ii) take such steps as the other Party reasonably requires it to take to mitigate the detrimental effects of any such breach or suspected breach on any of the Data Subjects and/or on the other Party; and (iii) otherwise cooperate with the other Party in investigating and dealing with such breach or suspected breach and its consequences.

2.3 The rights conferred under this Clause 3 are without prejudice to any other rights and remedies for breach of this Agreement whether in contract or otherwise in law.

3 DURATION, REVIEW AND AMENDMENT

3.1 This Agreement shall come into force immediately on being executed by all the Parties and continue for #[***insert termination: this will be when Parties cease sharing data in terms of contractual relationship with each other***], unless terminated earlier by the Disclosing Party in accordance with Clause 4.5.

3.2 This Agreement will be reviewed one year after it comes into force and every two years thereafter until termination or expiry in accordance with its terms.

3.3 In addition to these scheduled reviews and without prejudice to Clause 4.5, the Parties will also review this Agreement and the operational arrangements which give effect to it, if any of the following events takes place:

3.3.1 the terms of this Agreement have been breached in any material aspect, including any security breach or data loss in respect of Data which is subject to this Agreement; or

3.3.2 the Information Commissioner or any of his or her authorised staff recommends that the Agreement be reviewed.

3.4 Any amendments to this Agreement will only be effective when contained within a formal amendment document which is formally executed in writing by both Parties.

3.5 In the event that the Disclosing Party has any reason to believe that the Data Recipient is in breach of any of its obligations under this Agreement, the Disclosing Party may at its sole discretion:

3.5.1 suspend the sharing of Data until such time as the Disclosing Party is reasonably satisfied that the breach will not re-occur; and/or

3.5.2 terminate this Agreement immediately by written notice to the Data Recipient if the Data Recipient commits a material breach of this Agreement which (in the case of a breach capable of a remedy) it does not remedy within five (5) Business Days of receiving written notice of the breach.

3.6 Where the Disclosing Party exercises its rights under Clause **Error! Reference source not found.**, it may request the return of the Data (in which case the Data

Recipient shall, no later than fourteen (14) days after receipt of such a written request from the Disclosing Party, at the Disclosing Party's option, return or permanently erase/destroy all materials held by or under the control of the Data Recipient which contain or reflect the Data and shall not retain any copies, extracts or other reproductions of the Data either in whole or in part and shall confirm having done so to the other Party in writing), save that the Data Recipient will be permitted to retain one copy for the purpose of complying with, and for so long as required by, any law or judicial or administrative process or for its legitimate internal compliance and/or record keeping requirements.

4 LIABILITY

4.1 Nothing in this Agreement limits or excludes the liability of either Party for:

4.1.1 death or personal injury resulting from its negligence; or
4.1.2 any damage or liability incurred as a result of fraud by its personnel; or
4.1.3 any other matter to the extent that the exclusion or limitation of liability for that matter is not permitted by law.

4.2 The Data Recipient indemnifies the Disclosing Party against any losses, costs, damages, awards of compensation, any monetary penalty notices or administrative fines for breach of Data Protection Law and/or expenses (including legal fees and expenses) suffered, incurred by the Disclosing Party, or awarded, levied or imposed against the other party, as a result of any breach by the Data Recipient of its obligations under this Agreement. Any such liability arising from the terms of this Clause 5.2 is limited to £# (# STERLING) in the aggregate for the duration of this Agreement.

4.3 Subject to Clauses **Error! Reference source not found.** and **Error! Reference source not found.** above:

4.3.1 each Party excludes all liability for breach of any conditions implied by law (including any conditions of accuracy, security, completeness, satisfactory quality, fitness for purpose, freedom from viruses, worms, trojans or other hostile computer programs, non-infringement of proprietary rights and the use of reasonable care and skill) which but for this Agreement might have effect in relation to the Data;
4.3.2 neither Party shall in any circumstances be liable to the other party for any actions, claims, demands, liabilities, damages, losses, costs, charges and expenses that the other party may suffer or incur in connection with, or arising (directly or indirectly) from, any use of or reliance on the Data provided to them by the other Party; and
4.3.3 use of the Data by both Parties is entirely at their own risk and each party shall make its own decisions based on the Data, notwithstanding that this Clause shall not prevent one party from offering clarification and guidance to the other party as to appropriate interpretation of the Data.

5 DISPUTE RESOLUTION

5.1 The Parties hereby agree to act in good faith at all times to attempt to resolve any dispute or difference relating to the subject matter of, and arising under, this Agreement.

5.2 If the Representatives dealing with a dispute or difference are unable to resolve this themselves within twenty (20) Business Days of the issue arising, the matter shall be escalated to the following individuals in Part 4 of the Schedule identified as escalation points who will endeavour in good faith to resolve the issue.

5.3 In the event that the Parties are unable to resolve the dispute amicably within a period of twenty (20) Business Days from date on which the dispute or difference was escalated in terms of Clause **Error! Reference source not found.**, the matter may be referred to a mutually agreed mediator. If the identity of the mediator cannot be agreed, a mediator shall be chosen by the Dean of the Royal Faculty of Procurators in Glasgow.

5.4 If mediation fails to resolve the dispute or if the chosen mediator indicates that the dispute is not suitable for mediation, and the Parties remain unable to resolve any dispute or difference in accordance with Clauses 6.1 to 6.3, then either Party may, by notice in writing to the other Party, refer the dispute for determination by the courts in accordance with Clause 8.

5.5 The provisions of Clauses 6.1 to 6.4 do not prevent either Party from applying for an interim court order whilst the Parties attempt to resolve a dispute.

6 NOTICES

6.1 Any Notices to be provided in terms of this Agreement must be provided in writing and addressed to the relevant Party in accordance with the contact details noted in Part 4 of the Schedule, and will be deemed to have been received (i) if delivered personally, on the day of delivery; (ii) if sent by first class post or other next working day delivery, the second day after posting; (iii) if by courier, the date and time the courier's delivery receipt if signed; or (iv) if by fax, the date and time of the fax receipt.

7 GOVERNING LAW

7.1 This Agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) (a **"Dispute"**) shall, in all respects, be governed by and construed in accordance with the law of Scotland. Subject to Clause 6, the Parties agree that the Scottish Courts shall have exclusive jurisdiction in relation to any Dispute.

IN WITNESS WHEREOF these presents consisting of this and the preceding 6 pages together with the Schedule in 6 parts hereto are executed by the Parties hereto as follows:

On behalf of the association
at

on
by

Print Full Name	Director/Secretary/Authorised Signatory

before this witness

Print Full Name	Witness

Address

On behalf of #[Party 2]
at

on
by

Print Full Name	Director/Secretary/Authorised Signatory

before this witness

Print Full Name	Witness

Address

THIS IS THE SCHEDULE REFERRED TO IN THE FOREGOING DATA SHARING AGREEMENT BETWEEN THE ASSOCIATION AND #[PARTY 2]

SCHEDULE PART 1 – DATA

Drafting Note: This Part should contain details of the Personal Data to be shared between Parties and will need to be populated on a case-by-case basis when utilising this Agreement.

DATA SUBJECTS

For the purposes of this Agreement, Data Subjects are all living persons about whom information is transferred between the Parties.

SCHEDULE PART 2: PURPOSE AND LEGAL BASIS FOR PROCESSING

Purpose
The Parties are exchanging Data to allow #[insert details].

Legal Basis
#[insert details - this will require specific requirements to be drafted in to the model Agreement depending on the relationship between the Association and Party 2]

SCHEDULE PART 3 - DATA TRANSFER RULES

Information exchange can only work properly in practice if it is provided in a format which the Data Recipient it can utilise. It is also important that the Data is disclosed in a manner which ensures that no unauthorised reading, copying, altering or deleting of personal data occurs during electronic transmission or transportation of the Data. The Parties therefore agree that to the extent that data is physically transported, the following media are used:

- Face to face
- Secure email
- Courier
- Encrypted removable media
- #[**insert further methods of transport of Data (and delete above if desired)**]

The data is encrypted, with the following procedure(s):

- #[**insert details**]

SCHEDULE PART 4 – REPRESENTATIVES

Contact Details

Association
Name:
Job Title:
Address:
E-mail:
Telephone Number:

#[Party 2]
Name:
Job Title:
Address:
E-mail:
Telephone Number:

SCHEDULE PART 5 – SECURITY MEASURES

1 The Parties shall each implement an organisational information security policy.

2 Physical Security

2.1 Any use of data processing systems by unauthorised persons must be prevented by means of appropriate technical (keyword / password protection) and organisational (user master record) access controls regarding user identification and authentication. Any hacking into the systems by unauthorised persons must be prevented. Specifically, the following technical and organisational measures are in place:

The unauthorised use of IT systems is prevented by:

- User ID
- Password assignment
- Lock screen with password activation
- Each authorised user has a private password known only to themselves
- Regular prompts for password amendments [Delete/amend as appropriate]

The following additional measures are taken to ensure the security of any Data:

- Network Username
- Network Password
- Application Username
- Application Password
- Application Permissions and access restricted to those who require it *(Drafting Note: though this is no longer recommended so individual members may wish to delete)*
  [Delete/ amend as appropriate]

3 Disposal of Assets

3.1 Where information supplied by a Party no longer requires to be retained, any devices containing Personal Data should be physically destroyed or the information should be destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function.

4 Malicious software and viruses

Each Party must ensure that:

4.1.1 PCs used in supporting the service are supplied with anti-virus software and anti-virus and security updates are promptly applied.

4.1.2 All files received by one Party from the other are scanned to ensure that no viruses are passed.

4.1.3 The Parties must notify each other of any virus infections that could affect their systems on Data transfer.

SCHEDULE PART 6 – DATA GOVERNANCE

Data accuracy

The Disclosing Party shall make reasonable efforts to ensure that Data provided to the Data Recipient is accurate, up-to-date and relevant.

In the event that any information, in excess of information reasonably required in order to allow both organisations to comply with their obligations, is shared, the Data Recipient will notify the other party immediately and arrange the secure return of the information and secure destruction of any copies of that information.

Data retention and deletion rules

The Parties shall independently determine what is appropriate in terms of their own requirements for data retention.

Both Parties acknowledge that Data that is no longer required by either organisation will be securely removed from its systems and any printed copies securely destroyed.

APENDIX 5 – MODEL DATA PROTECTION ADDENDUM

[Drafting Note: It is anticipated that specific standard clauses will require to be included within finalised DP Addendums depending on the third party processor and nature of the member's relationship with them, in which case this draft will require to be updated to reflect that]

DATA PROTECTION ADDENDUM

between

Ayrshire Housing, a Scottish Charity (Scottish Charity Number SC027906), registered in terms of the Companies Acts with registered number (185652) and having its registered office/main office at 119 Main Street, AYR, KA8 8BX ("the association);

and

#[Insert organisation name, a # [e.g. Company] registered in terms of the Companies Acts with registered number *[registered number]* and having its registered office/main office at #[*address]*] (the "Processor")

(each a "**Party**" and together the "**Parties**")

WHEREAS

[Drafting Note: Further detail will require to be inserted here to confirm relationship between Parties to the Agreement. This will depend on the precise nature of relationship so will require to be adapted for every individual use of this model Agreement.]

(a) The association and the Processor have entered in to an agreement/ contract to #[insert detail] (hereinafter the "Principal Agreement"/"Principal Contract");

(b) This Data Protection Addendum forms part of the Principal Agreement/Principal Contract (*delete as appropriate); and

(c) In consideration of the mutual obligations set out herein, the Parties hereby agree that the terms and conditions set out below shall be added as an Addendum to the Principal Agreement. Except where the context requires otherwise, references in this Addendum to the Principal Agreement are to the Principal Agreement as amended by, and including, this Addendum.

1. Definitions

1.1 The terms used in this Addendum shall have the meanings set forth in this Addendum. Capitalised terms not otherwise defined herein shall have the meaning given to them in the Principal Agreement. Except as modified below, the terms of the Principal Agreement/Contract shall remain in full force and effect. In this Addendum, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

1.1.1 **"Applicable Laws"** means (a) Data Protection Act 2018 (DPA 2018), (b) the UK General Data Protection Regulation ("GDPR"); and (c) any other applicable law with respect to any Association Personal Data in respect

of which any Company Group Member is subject to any other Data Protection Laws;

1.1.2 "**Association Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of the Association pursuant to or in connection with the Principal Agreement/Contract;

1.1.3 "**Contracted Processor**" means Processor or a Sub-processor;

1.1.4 "**Data Protection Laws**" means UK Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country;

1.1.5 "**EEA**" means the European Economic Area;

1.1.6 "**GDPR**" means UK General Data Protection Regulation;

1.1.7 "**Restricted Transfer**" means:

1.1.7.1 a transfer of Association Personal Data from the Association to a Contracted Processor; or

1.1.7.2 an onward transfer of Association Personal Data from a Contracted Processor to a Contracted Processor, or between two establishments of a Contracted Processor,

in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws);

1.1.8 "**Services**" means the services and other activities to be supplied to or carried out by or on behalf of the Processor for the Association pursuant to the Principal Agreement/ Contract;

1.1.9 "**Subprocessor**" means any person (including any third party but excluding an employee of Processor or any of its sub-contractors) appointed by or on behalf of Processor which is engaged in the Processing of Personal Data on behalf of the Association in connection with the Principal Agreement/Contract; and

1.2 The terms, "**Commission", "Controller", "Data Subject", "Personal Data", "Personal Data Breach", "Processing**" and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and their related terms shall be construed accordingly.

1.3 The word "include" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. Processing of Association Personal Data

2.1 The Processor shall:

2.1.1 comply with all applicable Data Protection Laws in the Processing of Association Personal Data; and

2.1.2 not Process Association Personal Data other than on the Association's documented **instructions ["of" insert Association staff member details**

here if appropriate] unless Processing is required by Applicable Laws to which the relevant Contracted Processor is subject, in which case the Processor shall to the extent permitted by Applicable Laws inform the Association of that legal requirement before the relevant Processing of that Personal Data.

2.2 The association

2.2.1 Instructs the Processor (and authorises Processor to instruct each Sub-processor) to:

2.2.1.1 Process Association Personal Data; and
2.2.1.2 in particular, transfer Association Personal Data to any country or territory.

as reasonably necessary for the provision of the Services and consistent with the Principal Agreement/Contract; and

2.2.2 warrants and represents that it is and will at all relevant times remain duly and effectively authorised to give the instruction set out in section 2.2.1.

2.3 The Schedule to this Addendum sets out certain information regarding the Contracted Processors' Processing of the Association Personal Data as required the GDPR (and, possibly, equivalent requirements of other Data Protection Laws). The Association may make reasonable amendments to the Schedule by written notice to Processor from time to time as the Association reasonably considers necessary to meet those requirements. Nothing in the Schedule (including as amended pursuant to this section 2.3) confers any right or imposes any obligation on any party to this Addendum.

3. Processor and Personnel

The Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Association Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Association Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Applicable Laws in the context of that individual's duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall in

relation to the Association Personal Data implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in the GDPR.

4.2 In assessing the appropriate level of security, the Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5. Subprocessing [*Drafting Note: This clause should be adjusted depending on the arrangements between Parties*]

5.1 The Association authorises the Processor to appoint (and permit each Subprocessor appointed in accordance with this section 5 to appoint) Subprocessors in accordance with this section 5 and any restrictions in the Principal Agreement.

5.2 The Processor may continue to use those Subprocessors already engaged by the Processor as at the date of this Addendum, subject to the Processor in each case as soon as practicable meeting the obligations set out in section 5.4.

5.3 The Processor shall give the Association prior written notice of its intention to appoint a Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. The Processor shall not appoint (nor disclose any Association Personal Data to) the proposed Subprocessor except with the prior written consent of the Association.

5.4 With respect to each Subprocessor, the Processor or the relevant shall:

5.4.1 before the Subprocessor first Processes Association Personal Data (or, where relevant, in accordance with section 5.2), carry out adequate due diligence to ensure that the Subprocessor is capable of providing the level of protection for Association Personal Data required by the Principal Agreement;

5.4.2 ensure that the arrangement between on the one hand (a) the Processor, or (b) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, is governed by a written contract including terms which offer at least the same level of protection for Association Personal Data as those set out in this Addendum and meet the requirements in the GDPR;

5.4.3 if that arrangement involves a Restricted Transfer, ensure that the Standard Contractual Clauses are at all relevant times incorporated into the agreement between on the one hand (a) the Processor or (b) the relevant intermediate Subprocessor; and on the other hand the Subprocessor, or before the Subprocessor first Processes association Personal Data; and

[*Drafting Note: Each member organisation will require to check arrangements with its Data Processors to ascertain where the Processing is taking place – i.e. within UK or outwith. If outwith, where. The Standard Contractual Clauses are not appended to this initial draft for discussion as it is not anticipated that member organisations will be contracting with Data Processors who are Processing Personal Data outwith the UK*]

5.4.4 provide to the association for review such copies of the Contracted Processors' agreements with Subprocessors (which may be redacted to remove confidential commercial information not relevant to the requirements of this Addendum) as the association may request from time to time.

5.5 The Processor shall ensure that each Subprocessor performs the obligations under sections 2.1, 3, 4, 6.1, 7.2, 8 and 10.1, as they apply to Processing of Association Personal Data carried out by that Subprocessor, as if it were party to this Addendum in place of the Processor.

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, the Processor shall assist the Association by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Association's obligations to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 The Processor shall:

6.2.1 promptly notify the Association if any Contracted Processor receives a request from a Data Subject under any Data Protection Law in respect of Association Personal Data; and

6.2.2 ensure that the Contracted Processor does not respond to that request except on the documented instructions of the Association or as required by Applicable Laws to which the Contracted Processor is subject, in which case the Processor shall to the extent permitted by Applicable Laws inform the Association of that legal requirement before the Contracted Processor responds to the request.

7. Personal Data Breach

7.1 The Processor shall notify the Association without undue delay upon the Processor or any Subprocessor becoming aware of a Personal Data Breach affecting the Association Personal Data, providing the Association with sufficient information to allow it to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 The Processor shall co-operate with the Association and at its own expense take such reasonable commercial steps as are directed by the Association to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

The Processor shall provide reasonable assistance to the association with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which the Association reasonably considers to be required by the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Association Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9. Deletion or return of Association Personal Data

9.1 Subject to sections 9.2 and 9.3, the Processor shall promptly and in any event within seven (7) days of the date of cessation of any Services involving the Processing of Association Personal Data (the "Cessation Date"), delete and procure the deletion of all copies of those Company Personal Data.

9.2 Subject to section 9.3, the association may in its absolute discretion by written notice to the Processor within seven (7) days of the Cessation Date require the Processor to (a) return a complete copy of all Association Personal Data to the Association by secure file transfer in such format as is reasonably notified by the Association to the Processor; and (b) delete and procure the deletion of all other copies of Association Personal Data Processed by any Contracted Processor. The Processor shall comply with any such written request within seven (7) days of the Cessation Date.

9.3 Each Contracted Processor may retain Association Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws and always provided that the Processor shall ensure the confidentiality of all such Company Personal Data and shall ensure that such Company Personal Data is only Processed as necessary for the purpose(s) specified in the Applicable Laws requiring its storage and for no other purpose.

9.4 Processor shall provide written certification to the Association that it has fully complied with this section 9 within fourteen (14) days of the Cessation Date.

10. Audit rights

10.1 Subject to sections 10.2 and 10.3, the Processor shall make available the Association on request all information necessary to demonstrate compliance with this Addendum, and shall allow for and contribute to audits, including inspections, by the Association or an auditor mandated by the association in relation to the Processing of the Association Personal Data by the Contracted Processors.

10.2 Information and audit rights of the association only arise under section 10.1 to the extent that the Principal Agreement/Contract does not otherwise give them

information and audit rights meeting the relevant requirements of Data Protection Laws.

10.3 Where carrying out an audit of Personal Data, the association shall give the Processor reasonable notice of any audit or inspection to be conducted under section 10.1 and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the Contracted Processors' premises, equipment, personnel and business while its personnel are on those premises in the course of such an audit or inspection. A Contracted Processor need not give access to its premises for the purposes of such an audit or inspection:

10.3.1 to any individual unless they produce reasonable evidence of identity and authority; or

10.3.2 outside normal business hours at those premises, unless the audit or inspection needs to be conducted on an emergency basis and the Association undertaking an audit has given notice to the Processor that this is the case before attendance outside those hours begins.

11. General Terms

Governing law and jurisdiction

11.1 The Parties hereby submit to the choice of jurisdiction stipulated in the Principal Agreement/Contract with respect to any disputes or claims howsoever arising under this Addendum, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

11.2 this Addendum and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Principal Agreement/Contract.

Order of precedence

11.3 Nothing in this Addendum reduces the Processor's obligations under the Principal Agreement/Contract in relation to the protection of Personal Data or permits the Processor to Process (or permit the Processing of) Personal Data in a manner which is prohibited by the Principal Agreement/Contract.

11.4 Subject to section 11.2, with regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the parties, including the Principal Agreement/Contract and including (except where explicitly agreed otherwise in writing, signed on behalf of the parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.

[Drafting Note: see comments above re Restricted Transfers etc and the applicability of standard contractual clauses]

Changes in Data Protection Laws, etc.

11.5 The association may:

11.5.1 by giving at least twenty eight (28) days' written notice to the Processor, from time to time make any variations to the terms of the Addendum which are required, as a result of any change in, or decision of a competent authority under, that Data Protection Law, to allow those Restricted Transfers to be made (or continue to be made) without breach of that Data Protection Law; and

11.5.2 propose any other variations to this Addendum which the Association reasonably considers to be necessary to address the requirements of any Data Protection Law.

Severance

11.6 Should any provision of this Addendum be invalid or unenforceable, then the remainder of this Addendum shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

IN WITNESS WHEREOF, this Addendum is entered into and becomes a binding part of the Principal Agreement with effect from the date first set out above.

On behalf of the Association
at

on
by

Print Full Name	Director/Secretary/Authorised Signatory

before this witness

Print Full Name	Witness

Address

On behalf of the Processor
at

on

by

Print Full Name	Director/Secretary/Authorised Signatory

before this witness

Print Full Name	Witness

Address

SCHEDULE

This is the Schedule referred to in the foregoing Data Protection Addendum between the Association and the Processor

Part 1 – Data and Categories of Data Subject

For the purposes of this Data Protection Addendum, the categories of personal or special categories of data being processed are:

Name, Address, Contact Details, Household makeup, language spoken, vulnerabilities or risk factors (including deafness, mental health, physical disability), criminal record, associates [#amend as necessary]

The data subjects will be tenants of the Association and members of the tenant's household.

Part 2 – Nature and purpose of the processing

The Processor will processes Association Personal Data when performing housing management and void management tasks in accordance with the Management Agreement. [#amend as necessary]

Parties are processing this data for the following reasons:

the processing is necessary for the performance of the contracts between the Association and its tenants.

[#add additional grounds as necessary]

Part 3 – Duration and subject-matter

The subject matter of this Agreement is the execution and performance of the services specified within the Management Agreement, performed by the Processor as Data Processor. [#amend as necessary]

The Agreement will remain in place until terminated or until the [#insert principal contract details] is terminated, whichever is earlier. [#amend as necessary]

Part 4 – Representatives

The Association has an appointed DPO for data protection matters. This contact must be contacted should the Processor;

(a) receive a Data Subject Access request
(b) identify or become aware of a Personal Data Breach.

The Processor requires to provide contact details below of their Data Protection Officer (if applicable) or appropriate contact person in relation to this addendum.

Contact Details

Association Contact 1 (#insert DPO details)

Name: :
Job Title:
Address:
Email:
Telephone:

Association Contact 2

Name: :
Job Title:
Address:
Email:
Telephone:

Processor Contact 1

Name:
Job Title:
Address:
Email:
Telephone:

Processor Contact 1

Name:
Job Title:
Address:
Email:
Telephone:

Ayrshirehousing

DATA PROTECTION PERIODS

The table below gives retention periods for Personal Data held and processed by the association. It is intended to be used as a guide only. The association recognises that not all Personal Data can be processed and retained for the same duration, and retention will depend on the individual circumstances relative to the Data Subject whose Personal Data is stored.

Type of Record	Suggested Retention Time
Membership Records	5 years after last contact
Personal files including training records and notes of disciplinary and grievance hearings.	6 years to cover the time limit for bringing any civil legal action, including national minimum wage claims and contractual claims.
Redundancy details, calculations of payments, refunds, notification to the Secretary of State	6 years from the date of the redundancy.
Application forms, interview notes	Maximum a year from date of interviews. Successful applicant documents should be transferred to personal file.
Documents proving the right to work in the UK	2 years after employment ceases.
Facts relating to redundancies	6 years if less than 20 redundancies. 12 years if 20 or more redundancies.
Payroll	3 years after the end of the tax year they relate to.
Income tax, National Insurance returns, correspondence with the tax office	At least 3 years after the end of the tax year they relate to.
Retirement benefit schemes – notifiable events e.g., relating to incapacity	6 years from end of the scheme year in which the event took place.
Pensioners' records	12 years after the benefit ceases.
Statutory maternity/paternity and adoption pay records, calculations, certificates (MAT 1Bs) or other medical evidence	3 years after the end of the tax year to which they relate.
Parental leave	18 years from the birth of the child.
Statutory Sick Pay records calculations, certificates, and self-certificates.	3 years after the end of the tax year to which they relate.
Wages/salary records, expenses, bonuses	6 years.
Records relating to working time	2 years from the date they were made.

Accident books and records and reports of accidents	3 years after the date of the last entry; or if the accident involves a child/young adult, then until that person reaches 21 years of age.
Health and Safety assessments and records of consultations with safety representatives and committee	Permanently
Health records	During employment and 3 years thereafter if reason for termination of employment is connected to health.
Board member documents	5 years after cessation of membership.
Documents relating to successful tenders	5 years after end of contract.
Documents relating to unsuccessful form of tender	5 years after notification.
Applicants for accommodation	5 years.
Housing Benefits Notifications	Duration of Tenancy.
Tenancy Files	Duration of Tenancy.
Former Tenants' files (key info)	5 years.
Third party documents Re., care plans	Duration of Tenancy.
Records Re., offenders. Ex-offenders (sex offenders register)	Duration of Tenancy.
Lease Documents	5 years after lease termination.
ASB case files	5 years/end of legal action.
Board meetings/residents' meetings	1 year
Minute of factoring meetings	Duration of appointment.