This document is available in other languages or formats.
Please contact the office for details.

Policy:	Privacy Policy
Legal Requirements:	UK General Data Protection Regulation (UK GDPR); Data Protection Act 2018; Data (Use and Access) Act) 2025 (DUA); EU General Data Protection Regulation (EU GDPR); and The Privacy and Electronic (EC Directive) Regulations 2003.
Regulatory Standards:	The Scottish Housing Regulator has set out Regulatory Standards for all Registered Social Landlords (RSLs) to ensure that RSLs deliver good outcomes and services for its tenants and service users through good governance and financial management. This policy evidences that the following Regulatory Standards are being met: Standard 1. The governing body leads and directs the RSL to achieve good outcomes for its tenants and other service users. Standard 5. The RSL conducts its affairs with honesty and integrity.
Notifiable Events Guidance	In compiling this policy, consideration has been given to the Notifiable Events Guidance issued by the Scottish Housing Regulator and the impact of that guidance on the policy.
Equality and Diversity:	The Association is committed to Equal Opportunities and will endeavour to ensure that all services are carried out in an undiscriminating manner in line with the Association's Equality and Diversity Policy. In particular, the Association will not discriminate on the grounds of age, disability, marriage and civil partnership, pregnancy and maternity, race, religion or belief, gender, gender reassignment or sexual orientation.
Human Rights:	In compiling this policy, consideration has been given to "The Right to Adequate Housing" (Fact Sheet No. 21/Rev.1) published by the Office of the United Nations High Commissioner for Human Rights and the impact of that guidance on the policy. In particular, the Association is satisfied that this policy promotes the key aspects of the right to adequate housing – that it contains freedoms; entitlements; provides more than four walls and a roof; and protects against forced evictions.
Complaints:	Although the Association is committed to providing high levels of service, we accept that there may be occasions where customers may not be satisfied with the service they have received. The Association values all complaints and uses this information to improve the services that it provides. The Association's Complaints Policy describes our complaints handling procedure and how to make a complaint.
General Data Protection Regulation (GDPR):	The Association will treat all customers' personal data in line with its obligations under the current data protection regulations and our Privacy Policy. Information regarding how data will be used and the basis for processing data is provided in the Association's Fair Processing Notice.
Policy Author:	Kevin Freeman
Policy Review:	In order to ensure that any change in circumstances is accommodated this policy will be subject to review every three years in the month of March.
Policy Approval:	This policy was last reviewed / approved by the Management Committee of Yoker Housing Association Limited at its meeting held on Thursday the 28th of May 2026.

Introduction

Yoker Housing Association Limited (hereinafter the "Association") is committed to ensuring the secure and safe management of data held by the Association in relation to customers, 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 customers (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. This data contains Personal Data and Sensitive Personal Data (known as Special Categories of Personal Data under the 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.

Statement of Aims

The aim of this policy is to outline the Association's duties in processing Personal Data and to set out the procedures to be adopted for the management of such data.

Legal Requirements

It is a legal requirement that the Association must collect, handle and store personal information in accordance with the relevant legislation.

The relevant legislation in relation to the processing of data is:

- The UK General Data Protection Regulation ("the GDPR");
- The Privacy and Electronic Communications (EC Directive) Regulations 2003 ;
- The Data Protection Act 2018 ("the 2018 Act");
- Data (Use and Access) Act 2025 (DUA); and
- any legislation that, in respect of the United Kingdom, replaces, or enacts into United Kingdom domestic law, the UK GDPR, the Privacy and Electronic Communications (EC Directive) Regulations 2003 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.

The Association has a legal requirement to process data correctly. In order to meet this requirement the Association must collect, handle and store personal information in accordance with relevant legislation.

Data

The Association holds a variety of Data relating to living individuals, including customers and employees (also referred to as Data Subjects). Data which can identify Data Subjects and relates to them is known as Personal Data. The Personal Data held and processed by the Association is detailed within the Fair Processing Notices (Appendices 1 & 2) and the Data Protection Addendum of the Terms of and Conditions of Employment (Appendix 3) which has been provided to all employees.

"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 and which relates to that individual.

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". The Secretary of State may designate further categories of Special Category Personal Data and if this occurs the Association shall treat any such designated data accordingly.

Processing of Personal Data

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 refer to the "Consent" section in this policy);
- 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;
- Processing is necessary for the purposes of the legitimate interests pursued by the Association or by a third party; or
- Processing is necessary for the purposes of a recognised legitimate interest.

Fair Processing Notice

The Association has produced a Fair Processing Notice (FPN) which it is required to provide to all customers whose Personal Data is held by the Association. That FPN must be provided to the customer from the outset of processing their Personal Data and they should be advised of the terms of the FPN when it is provided to them. If the Association receives Personal Data about an individual from another source (so not from the individual direct) the Association will provide the required privacy information in accordance with the requirements of Data Protection Law.

The Fair Processing Notice (Appendix 1) sets out the Personal Data processed by the Association and the basis for that processing. This document is provided to all of the Association's customers at the outset of processing their data

Employees

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 the Employee Fair Processing Notice (Appendix 2) which is provided to prospective Employees at application stage. In the case of existing employees the Employee Fair Processing Notice should also be provided to employees along with the Contract of Employment Data Protection Clause (Appendix 3).

A copy of any employee's Personal Data held by the Association is available upon request by that employee from the Association's Data Protection Officer, subject to certain exemptions.

Consent

Consent as a ground of processing will require to be used from time to time by the Association when processing Personal Data. It should 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 (unless extenuating circumstances apply). The consent provided by the Data Subject must be freely given and the Data Subject will be required to sign a relevant consent form if willing to consent (again, subject to extenuating circumstances such as the Data Subject being unable to write). Any consent to be obtained by the Association must be for a specific and defined purpose (i.e. general consent cannot be sought). Where consent is being relied on, Data Subjects are free to withhold their consent or withdraw it at any future time.

Processing of Special Category Personal Data or Criminal Offence Data

In the event that the Association processes Special Category Personal Data or Criminal Offence Data, the Association must rely on an additional ground for processing in accordance with one of the special category grounds. These include, but are not restricted to, the following:

- 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, social security or social protection law;
- Processing is necessary for health or social care;
- 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 of Special Category Personal Data or Criminal Offence Data (continued)

- 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 under law

All the grounds for processing sensitive Personal Data are set out in the GDPR and expanded on in the Data Protection Act 2018.

Data Sharing

The Association shares its data with various third parties for numerous reasons in order that its day-to-day activities are 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 may require the third party organisations to enter in to an Agreement with the Association governing the processing of data, security measures to be implemented, and responsibility for breaches. There is a Model Data Sharing Agreement (Appendix 4) of this policy which the Association may use in such scenarios. However the Association will determine on a case-by-case basis what the most appropriate contract terms (if required) shall be.

Processors

A processor is a third-party entity that processes Personal Data on behalf of the Association and are frequently engaged if certain of the Association's work is outsourced (e.g. payroll, maintenance and repair works).

A processor must comply with Data Protection laws. The Association's 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.

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

Where the Association contracts with a third party to process Personal Data held by the Association, it shall require the third party to enter in to a written contract with the Association with such contract outlining, amongst other things, how Personal Data will be kept safe and secure. The Association has a model Data Protection Addendum set out in Appendix 5 to this policy and model Data Processing Clauses set out in Appendix 6 to this policy which can be used in these scenarios. However, the Association may, on a case-by-case basis, determine that other contract wording is appropriate.

Data Storage and Security

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

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 ensure that no Personal Data is left in a place where unauthorised personnel can access it. When the Personal Data is no longer required (and the Association has a Retention Policy which sets out the expected timescales for holding various personal categories of Personal Data) it must be disposed of by the employee so as to ensure its secure destruction. If the Personal Data requires to be retained on a physical file then the employee should ensure that it is affixed to the file which is then stored in accordance with the Association's storage provisions.

Electronic Storage - Personal Data stored electronically must also be protected from unauthorised use and access. Personal Data should be password protected when being sent internally or externally to the Association's processors or those with whom the Association has entered in to a Data Sharing Agreement. If Personal Data is stored on removable media (CD, DVD, USB memory stick) then that removable media must be encrypted and stored securely at all times when not being used. Personal Data should not be saved directly to mobile devices and should be stored on designated drivers and servers.

Breaches

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 this policy (refer to "Reporting to the ICO" section of this policy).

Breaches (Continued)

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 it becomes known the breach or potential breach has occurred, the Association's 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 must seek to contain the breach by whichever means available;
- The DPO must consider whether the breach is one which requires to be reported to the Information Commissioner's Office (ICO) and to the Data Subjects affected and, if appropriate, will do so in accordance with this policy; and
- Notify third parties in accordance with the terms of any applicable Data Sharing Agreements, Data Processing Agreements or equivalent contract terms.

Reporting to the Information Commissioner's Office (ICO) and to Data Subjects

The DPO will require to report any breaches which pose a risk to the rights and freedoms of the Data Subjects who are subject of the breach to the Information Commissioner's Office (ICO) within seventy-two hours of the breach occurring or the Association becoming aware of the breach. The DPO must also consider whether it is appropriate to notify those Data Subjects affected by the breach.

Where a breach poses a *high* risk to the rights and freedoms of the Data Subjects impacted by the breach, the Association must, in addition to notifying the ICO, promptly notify the Data Subjects in question.

Data Protection Officer ("DPO")

A Data Protection Officer is an individual who has an over-arching responsibility and oversight over compliance by the Association with Data Protection laws. The Association has appointed a Data Protection Officer (DPO). The Association's DPO's details are noted on the Association's website and contained within the Fair Processing Notices (Appendices 1 & 2).

The Data Protection Officer is responsible for:

- Monitoring the Association's compliance with Data Protection laws and this Policy and advising on compliance as needed;
- Co-operating with and serving as the Association's contact for discussions with the ICO; and
- Reporting breaches or suspected breaches to the ICO and data subjects in accordance with the Breaches Section of this policy.

Data Subject Rights

Certain rights are provided to Data Subjects under Data Protection Law:

- A right to be informed about the collection and use of their Personal Data (typically fulfilled by providing individuals with a Fair Processing Notice) (the "right to be informed");
- A right to access and receive a copy of their Personal Data, plus other supplementary information (the "right of access");
- A right to have inaccurate Personal Data rectified and incomplete Personal Data completed (the "right to rectification");
- A right to have Personal Data erased (the "right to erasure");
- The right to request the restriction or suppression of Personal Data (the "right to restrict");
- The right to obtain and reuse certain Personal Data across different providers (the "right to data portability");
- The right, in certain circumstances, to object to the processing of their Personal Data (the "right to object");
- The right to make a complaint about how their Personal Data has been processed (the "right to complain"); and
- Rights to protect individuals against automated decision making or profiling ("rights related to automated decision making").

These rights are notified to the Association's tenants and other customers in the Association's Fair Processing Notice. Such rights are subject to qualification and are not absolute.

Data Subject Rights (Continued)

The Right of Access: Subject Access Requests

Data Subjects are permitted to view their Personal Data held by the Association upon making a request to do so (a Subject Access Request) subject to certain exemptions. Upon receipt of a request by a Data Subject, the Association must respond to the Subject Access Request within one month from the day after the date of receipt of the request (unless the Association is entitled under the relevant legislation to increase this timescale). The Association:

- Must provide the data subject with an electronic or hard copy of the Personal Data requested, unless any exemption to the provision of that data applies in law.
- Where the Personal Data comprises of data relating to other Data Subjects the Association shall only release that data where: the Association has obtained consent from those Data Subjects or the Association determines it is reasonable to disclose said data without consent. or
- Where the Association does not hold the Personal Data sought by the Data Subject, must confirm that it does not hold any or that Personal Data sought to the Data Subject as soon as practicably possible, and in any event, not later than one month from the day after the date on which the request was made.

The Right to Erasure

A Data Subject can exercise their right to erasure (otherwise known as the right to be forgotten) by submitting a request to the Association seeking that the Association erase the Data Subject's Personal Data in its entirety.

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.

Requests for erasure will be considered and responded to by the Association within one month from the day after the date we receive the request unless the Association is entitled to increase the timescales under relevant legislation.

The Right to Restrict or Object to Processing

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

In the event that any direct marketing is undertaken from time-to-time by 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 must do so immediately.

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.

The Right to Rectification

A Data Subject may request the Association to have inaccurate Personal Data rectified. If appropriate, a Data Subject may also request the Association to have incomplete Personal Data completed.

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.

The Right to Data Portability

A Data Subject may ask for their Personal Data which they have provided to the Association to be provided in a structured, commonly used, machine readable format or the Data Subject may ask for this data to be transmitted directly to another organisation. This is subject to certain exemptions.

Data Subject Rights (Continued)

The Right to Data Portability (continued)

Each request received by the Association will to be considered on its own merits and, in some cases, legal advice will be required. The DPO will have responsibility for accepting or refusing the Data Subject's request and will respond in writing to the request.

The Right to Complain

A Data Subject may complain to the Association if they consider their Personal Data has been processed by the Association in contravention of Data Protection Law.

Any such complaint shall be handled in accordance with the Association's Data Protection Complaints Process (Appendix 7).

Rights Related to Automated Decision Making

Should the Association utilise any automated decision making it shall follow the requirements set down in data protection law to protect the Data Subjects in question.

Privacy Impact Assessments (PIAs)

These are a means of assisting the Association in identifying and reducing the risks that our operations have on personal privacy of Data Subjects. Whilst this policy uses the term PIAs, it is also recognised that these assessments are also commonly referred to as "Data Protection Impact Assessments" or similar.

The Association shall:

- 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
- 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 are required to be taken to protect the Personal Data.

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

Archiving, Retention and Destruction of Data

The Association cannot store and retain Personal Data indefinitely. It must ensure that Personal Data is only retained for the period necessary. The Association shall ensure that all Personal Data is archived and destroyed in accordance with the periods specified within Appendix 8 of this policy.

List of Appendices

1. Fair Processing Notice
2. Employee Fair Processing Notice
3. Contract of Employment (Data Protection Clause)
4. Data Sharing Agreement
5. Data Protection Addendum
6. Data Processing Clauses
7. Data Protection Complaints Process
8. Data Retention Periods

This notice explains what information we collect, when we collect it and how we use this. During the course of our activities we will process personal data (which may be held on paper, electronically, or otherwise) about you and we recognise the need to treat it in an appropriate and lawful manner. The purpose of this notice is to make you aware of how we will handle your information.

Who are we

Yoker Housing Association Limited, a Scottish Charity (Scottish Charity Number SC036604), a registered society under the Co-operative and Community Benefit Societies Act 2014 with Registered Number 1998RS and having their Registered Office at 2310 Dumbarton Road, Yoker, Glasgow, G14 0JS ("we" or "us") take the issue of security and data protection very seriously and strictly adhere to guidelines published in the UK GDPR and Data Protection Act (2018 Act) together with any domestic laws subsequently enacted.

We are registered as a Controller with the Office of the Information Commissioner (ICO) under registration number Z6291362 and we are the controller of any personal data that you provide to us.

Our Data Protection Officer is Kevin Freeman. Any questions relating to this notice and our privacy practices should be addressed to our Data Protection Officer, at our Registered Office at 2310 Dumbarton Road, Yoker, Glasgow, G14 0JS. Alternatively, our Data Protection Officer can be contacted by telephone on 0141 950 9052.

How we collect information from you and what information we collect

We collect information about you to enable us to perform our contractual obligations. You, in turn, are under a contractual obligation to provide the data requested from you to enable performance of the contract (i.e. the tenancy agreement you are party to):

- When you apply for housing with us, become a tenant, request services / repairs, enter into a factoring agreement with ourselves howsoever arising or otherwise provide us with your personal details;
- When you apply to become a member;
- From your use of our online services, whether to report any tenancy / factor related issues, apply for housing, make a complaint or otherwise; and
- From your arrangements to make payment to us (such as bank details, payment card numbers, employment details, benefit entitlement and any other income and expenditure related information).

Under the terms of the tenancy agreement / factoring agreement / housing application form, you are required to provide us with the following information:

- Name;
- Address;
- Telephone number;
- E-mail address;
- National Insurance Number;
- Next of Kin;
- Demographic information.

We receive the following information from third parties:

- Benefits information, including awards of Housing Benefit / 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 behavior.

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

We need your information and will use your information to undertake and perform our obligations and duties to you in accordance with the terms of our contract with you. This includes:

- To enable us to supply you with the services and information which you have requested;
- To enable us to respond to your repair request, housing application and complaints made;
- To analyse the information we collect so that we can administer, support and improve and develop our business and the services we offer;
- To contact you in order to send you details of any changes to our services or supplies which may affect you;
- For all other purposes consistent with the proper performance of our operations and business; and
- To contact you for your views on our products and services.

The information you provide to us will be treated by us as confidential and will be processed only by our employees within the UK. We may disclose your information to other third 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 business entity, your information may be disclosed to our new or prospective business partners or owners;
- If we instruct repair or maintenance works, your information may be disclosed to any contractor;
- If we are investigating a complaint, information may be disclosed to Police Scotland, Local Authority departments, Scottish Fire & Rescue Service and others involved in any complaint, whether investigating the complaint or otherwise;
- If we are updating tenancy details, your information may be disclosed to third parties (such as utility companies and the Local Authority);
- If we are investigating payments made or otherwise, your information may be disclosed to payment processors, Local Authority and the Department for Work & Pensions;
- If we are conducting a survey of our products and / or service, your information may be disclosed to third parties assisting in the compilation and analysis of the survey results.

Unless we have a lawful basis for disclosure, we will not otherwise share, sell or distribute any of the information you provide to us without your consent.

Transfers outside the UK

The Association will only store personal information within the UK. However, we may transfer your information outside the UK. Where information is transferred outside the UK we ensure that there are adequate safeguards in place to protect your information in accordance with this notice.

Security

When you give us information we take steps to make sure that your personal information is kept secure and safe. The following security processes are undertaken to ensure that personal information is kept secure:

- Paper records are only stored in designated areas within the Association's office. All areas where personal information is kept are locked to prevent unauthorised access;
- Electronic records are stored on the Association's server. The server is kept in a locked room to prevent unauthorised access;
- Electronic records are password protected and can only be accessed by authorised personnel; and
- Electronic records are backed up daily. These records are backed up onto encrypted hard drives. The Association does not use clouds to back up or store personal information.

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 (we may be legally required to hold some types of information), or as set out in any relevant contract we have with you.

We will generally keep your information for the minimum periods set out in our Data Retention Schedule contained within our Privacy Policy after which this will be destroyed if it is no longer required for the reasons it was obtained.

Our full retention schedule is detailed within our Privacy Policy. You can obtain a copy of this policy at the Association's office or on our website.

Your Rights

You have the right at any time to:

- Ask for a copy of the information about you held by us in our records;
- Require us to correct any inaccuracies in your information;
- Request that we restrict your data processing or object to our processing in certain circumstances;
- Data portability (in certain circumstances);
- Make a request for us to delete what personal data of yours that we hold;
- Object to receiving any marketing communications from us; and
- Submit a complaint to us if you believe your personal data has been handled in a way that does not comply with data protection law.

If you would like to exercise any of your rights above please contact us:

- By telephone on 0141 950 9052
- By Email to housing@yokerha.org.uk
- Or write to us at: Data Protection Officer, Yoker Housing Association Limited, 2310 Dumbarton Road, Yoker, Glasgow, G14 0JS

You should note that your rights under the UK GDPR and 2018 Act are not absolute and are subject to qualification.

In addition you have certain rights where we use automated decision making in respect of you or your personal data and will inform you of any such processing and those rights should we use any such processes.

If you have any complaints about the way your data is processed or handled by us, please contact our Data Protection Officer:

- By Email to housing@yokerha.org.uk
- Or write to us at: Data Protection Officer, Yoker Housing Association Limited, 2310 Dumbarton Road, Yoker, Glasgow, G14 0JS

If you remain unsatisfied after your complaint has been processed by us, you also have the right to complain to the Information Commissioner's Office (ICO) in relation to our use of your information. The Information Commissioner's contact details are noted below:

The Information Commissioner's Office – Scotland
6th Floor, Quartermile One, 15 Lauriston Place, Edinburgh EH3 9EP
Telephone: 0303 123 1113
Email: Scotland@ico.org.uk

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

This notice explains what information we collect, when we collect it and how we use this. During the course of our activities we will process personal data (which may be held on paper, electronically, or otherwise) about you and we recognise the need to treat it in an appropriate and lawful manner. The purpose of this notice is to make you aware of how we will handle your information.

Yoker Housing Association Limited ("we" or "us") is committed to a policy of protecting the rights of individuals with respect to the processing of their personal data and adhere to guidelines published in the UK GDPR and Data Protection Act (2018 Act) together with any domestic laws subsequently enacted. We collect and use personal data for a variety of reasons.

We are notified as a Controller with the Office of the Information Commissioner (ICO) under registration number Z6291362 and we are the controller of any personal data that you provide to us.

Any questions relating to this notice and our privacy practices should be addressed to our Data Protection Officer, Kevin Freeman at our Registered Office at 2310 Dumbarton Road, Yoker, Glasgow, G14 0JS. Alternatively, our Data Protection Officer can be contacted by telephone on 0141 950 9052.

We collect the following information from you through a variety of resources (i) directly from you; or (ii) third parties (including employment agencies, pensions services):

- Name;
- Date of Birth;
- Address;
- Telephone number;
- E-mail address;
- National Insurance number;
- Personal characteristics such as gender and ethnic group;
- Qualifications;
- Absence information; and
- Bank account information.

We collect and use the above information and personal data for:

- Administration of contracts of employment;
- Payment of salaries;
- Recruitment and selection;
- Pensions and associated benefits, appraisal, training and development; and
- Membership of professional bodies.

We may disclose and share information about you with third parties for the purposes set out in this notice, or for purposes approved by you, including the following:

- To process your monthly salary payments;
- To allow your pension provider to process pensions information and handle your pension;
- To allow your electronic payslips to be produced and issued to you; and
- If we enter into a joint venture with or is sold to or merged with another business entity, your information may be disclosed to our new business partners or owners.

The Association will only store personal information within the UK. However, we may transfer your information outside the UK. Where information is transferred outside the UK we ensure that there are adequate safeguards in place to protect your information in accordance with this notice.

When you give us information we take steps to make sure that your personal information is kept secure and safe. The following security process are undertaken to ensure that personal information is kept secure:

- Paper records are only stored in designated areas within the Association's office. All areas where personal information is kept are locked to prevent unauthorised access;
- Electronic records are stored on the Association's server. The server is kept in a locked room to prevent unauthorised access;
- Electronic records are password protected and can only be accessed by authorised personnel; and
- Electronic records are backed up daily. These records are backed up onto encrypted hard drives. The Association does not use clouds to back up or store personal 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 (we may be legally required to hold some types of information), or as set out in any relevant contract we have with you.

Data retention guidelines on the information we hold is provided in our Privacy Policy.

You have the right at any time to:

- Ask for a copy of the information about you held by us in our records;
- Ask us to correct any inaccuracies of fact in your information;
- Request that we restrict your data processing or object to our processing in certain circumstances;
- Data portability;
- Make a request for us to delete what personal data of yours we hold;
- Object to receiving any marketing communications from us; and
- Submit a complaint to us if you believe your personal data has been handled in a way that does not comply with data protection law.

These rights are qualified and are not absolute.

In addition you have certain rights where we use automated decision making in respect of you or your personal data and will inform you of any such processing and those rights should we use any such processes

If you would like to find out more about how we use your personal data or want to see a copy of information about you that we hold or wish to exercise any of your above rights, please contact the Association's Data Protection Officer, Kevin Freeman.

If you have any complaints about the way your data is processed or handled by us, please contact our Data Protection Officer:

- By Email to housing@yokerha.org.uk
- Or write to us at: Data Protection Officer, Yoker Housing Association Limited, 2310 Dumbarton Road, Yoker, Glasgow, G14 0JS

If you remain unsatisfied after your complaint has been processed by us, you also have the right to complain to the Information Commissioner's Office (ICO) in relation to our use of your information. The Information Commissioner's contact details are noted below:

The Information Commissioner's Office – Scotland
6th Floor, Quartermile One, 15 Lauriston Place, Edinburgh EH3 9EP
Telephone: 0303 123 1113
Email: Scotland@ico.org.uk

The accuracy of your information is important to us – please help us keep our records updated by informing us of any changes to your personal and contact details.

We hold information about you on your personal file. You are entitled to access this file and to other information that the Association holds about them, subject to certain restrictions imposed by the UK GDPR and Data Protection Act 2018. The Fair Processing Notice annexed to these Terms & Conditions (a duplicate copy of which we have provided to you) confirms what personal information we hold which we obtained from you or third parties. Our Privacy Policy contains further details regarding Data Protection matters, and the handling of personal data. By signing these Terms & Conditions you confirm that you have read and understood our Privacy Policy and will comply with the terms of that Policy.

We may also require to process sensitive personal data of yours. Any sensitive personal data we process to comply with our obligations as your employers and / or your vital interests is outlined within the Fair Processing Notice annexed to these Terms & Conditions. We will seek to obtain your consent to process any additional sensitive personal data of yours that we wish to process if appropriate.

For the purposes of the Legal Writings (Counterparts and Delivery) (Scotland) Act 2015, this Agreement is delivered on _____

DATA SHARING AGREEMENT

between

Yoker Housing Association Limited, a Scottish Charity (Scottish Charity Number SC036604), a registered society under the Co-operative and Community Benefit Societies Act 2014 with Registered Number 1998RS and having their Registered Office at 2310 Dumbarton Road, Yoker, Glasgow, G14 0JS (the "Data Discloser");

and

[**Full Company Name**] incorporated and registered [**Scotland**] with company number [**Number**] whose registered office is at [**Registered Office Address**] (the "**Data Receiver**")

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

WHEREAS

(a) The Data Discloser agrees to share the Personal Data with the Data Receiver in the UK on the terms set out in the Agreement.

(b) The Data Receiver agrees to use the Personal Data within the UK on the terms set out in this Agreement.

(c) This is a free-standing Agreement that does not incorporate commercial business terms established by the Parties under separate commercial arrangements.

NOW THEREFORE IT IS AGREED AS FOLLOWS:

1. DEFINITIONS AND INTERPRETATION

The following definitions and rules of interpretation apply in this Agreement

1.1 Definitions

Agreed Purposes: has the meaning given to it in Clause 2 of this Agreement.

Business Day: a day other than a Saturday, Sunday or public holiday in Scotland.

Data Protection Legislation: all applicable data protection and privacy legislation in force from time to time in the UK including without limitation the UK GDPR; the Data Protection Act 2018 (and regulations made thereunder) (DPA 2018); the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended; and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications).

Information Commission:

a) Until such times as section 118 of the Data (Use and Access) Act 2025 comes into force, the Information Commissioner (see Article 4(A3), UK GDPR and section 114, Data Protection Act 2018); or

b) From the commencement of section 118 of Data (Use and Access) Act 2025 the Information Commission (see section 117 of such Act and section 114A of the Data Protection Act 2018 (when in force)); or

c) Any successor bodies.

Personal Data Breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Shared Personal Data.

Shared Personal Data: the Personal Data to be shared between the Parties as set out in Clause 4 of this Agreement.

Subject Rights Requests: the exercise by a Data Subject of their rights under the Data Protection Legislation.

UK GDPR: has the meaning set out in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018.

1.2 **Controller, Processor, Data Subject** and **Personal Data, Processing** and **appropriate technical and organisational measures** shall have the meanings given to them in the Data Protection Legislation**.**

1.3 Clause and paragraph headings shall not affect the interpretation of this Agreement.

1.4 Unless the context otherwise requires, words in the singular shall include the plural and in the plural shall include the singular.

1.5 A reference to a company shall include any company, corporation or other body corporate, wherever and however incorporated or established.

1.6 A reference to a legislation or legislative provision shall include all subordinate legislation made from time to time under that legislation or legislative provision.

1.7 Any words following the terms including, include, in particular or for example or any similar expression shall be construed as illustrative and shall not limit the sense of the words, description, definition, phrase or term preceding those terms.

1.8 A reference to writing or written includes fax but not email.

2. PURPOSE

2.1 This Agreement sets out the framework for the sharing of Personal Data when one Controller (the Data Discloser) discloses Personal Data to another Controller (the Data Receiver). It defines the principles and procedures that the Parties shall adhere to and the responsibilities the Parties owe to each other.

2.2 The Parties consider this data sharing initiative necessary and proportionate as **[Describe Reasons(s)]**. The aim of the data sharing initiative is to **[Describe Aim(s)]**. It is fair as it will benefit **[individuals, the Parties or society]** by **[Describe Benefits]** and not unduly infringe the Data Subjects' fundamental rights and freedoms and interests.

2.3 The Data Recipient agrees to only Process Shared Personal Data, as described in Clause 4.1 for the following purposes:

a) **[Insert Purpose]**

b) **[Insert Purpose]**

[Add further sections as needed]

(the **Agreed Purposes**)

2.4 Each Party shall appoint a single point of contact (SPoC) who will work together to reach an agreement with regards to any issues arising from the data sharing and to improve actively the effectiveness of the data sharing initiative. The points of contact for each of the Parties are:

a) [**Insert for Data Discloser**]; and

b) [**Insert a Data Recipient**]

3. COMPLIANCE WITH DATA PROTECTION LAWS

3.1 Each Party must ensure compliance with applicable Data Protection Legislation at all times during this Agreement.

3.2 Each Party has such valid registrations **[[and] [or] has paid such fees]** as are required by the Information Commission.

4. SHARED PERSONAL DATA

4.1 The following types of Personal Data will be shared between the Parties during this Agreement:

a) [**Insert Category of Personal Data and Data Subjects**]

b) [**Insert Category of Personal Data and Data Subjects**]

c) [**Insert Category of Personal Data and Data Subjects**]

d) **[Add Further Sections as Needed and Data Subjects]**

The Shared Personal Data must not be irrelevant or excessive with regard to the Agreed Purposes.

5. LAWFUL FAIR AND TRANSPARENT PROCESSING

5.1 Each Party shall ensure that it Processes the Shared Personal Data fairly and lawfully.

5.2 Each Party shall ensure that it has legitimate grounds under the Data Protection Legislation for the Processing of Shared Personal Data.

5.3 The Parties each agree to provide such assistance as is reasonably required to enable the other Party to comply with Subject Rights Requests within the time limits imposed by the Data Protection Legislation.

5.4 The Data Discloser shall ensure that, prior to any Shared Personal Data (or any part) being transferred to the Data Receiver from time to time, each relevant Data Subject has been provided with clear and sufficient information (in an appropriate form) in accordance with Data Protection Legislation so as to enable fair, transparent and lawful Processing (including sharing) of the Shared Personal Data for the Agreed Purpose.

5.5 The Data Receiver undertakes to inform the Data Subjects, in accordance with the Data Protection Legislation, of the purposes for which it will process their Personal Data, the legal basis for such purposes and such other information as is required by the Data Protection Legislation.

6. DATA ACCURACY

6.1 The Data Discloser shall use all reasonable endeavours to ensure the accuracy of any Shared Personal Data prior to its disclosure to the Data Receiver in line with its obligations under Data Protection Legislation.

6.2 The Data Discloser makes no representation and gives no warranty (whether express or implied) that the Shared Personal Data will be suitable for the intended use by the Data Receiver.

6.3 Shared Personal Data must be limited to the Personal Data described in Clause 4.1. In the event the Data Recipient becomes aware that any Shared Personal Data extends beyond this it shall notify the Data Discloser without undue delay and arrange the secure return of any such Shared Personal Data.

7. DATA SUBJECTS' RIGHTS

7.1 Responsibility for compliance with and responding to any Subject Rights Request relating to the Shared Personal Data falls on the Party who received such Subject Rights Request.

7.2 The Data Discloser and Data Receiver each agree to provide such assistance as is reasonably required to enable the other Party to comply with Subject Rights Requests within the time limits imposed by the Data Protection Legislation for the duration of this Agreement.

8. DATA RETENTION AND DELETION

8.1 The Data Receiver shall not retain or process Shared Personal Data for longer than is necessary to carry out the Agreed Purpose.

8.2 Notwithstanding Clause 8.1, Parties shall continue to retain Shared Personal Data in accordance with any statutory or professional retention periods applicable in their respective countries and / or industry.

8.3 [Subject to Clause 8.5, The Data Receiver shall ensure that any Shared Personal Data is returned to the Data Discloser or destroyed on termination or expiry of this Agreement, at the option of the Data Discloser.

8.4 Following the deletion of Shared Personal Data in accordance with Clause 8.3, the Data Receiver shall notify the Data Discloser that the Shared Personal Data in question has been deleted in accordance with this Agreement.

8.5 If any law, regulation, or government or regulatory body requires the Data Receiver to retain any Shared Personal which would otherwise be required to be returned or destroyed, it will notify (to the extent is able to do so by law) the Data Discloser in writing of that retention requirement, giving details of the Shared Personal Data that it must retain, the legal basis for such retention, and establishing a specific timeline for return, deletion or destruction once the retention requirement ends.

8.6 Until the Data Receiver deletes or returns the Shared Personal Data in accordance with Clause 8.3 all requirements set out in this Agreement shall continue to apply to the Data Receiver for so long as the Shared Personal Data is processed by the Data Receiver.]

8.7 This Clause 8 shall survive termination of this Agreement.

9. TRANSFERS

9.1 For the purposes of this clause, transfers of Personal Data shall mean any sharing of Personal Data by the Data Receiver with a third party, and shall include the following:

a) Subcontracting the processing of Shared Personal Data;

b) Granting a third party Controller access to the Shared Personal Data.

9.2 If the Data Receiver appoints a third party Processor to Process the Shared Personal Data it shall comply with the relevant provisions of the Data Protection Legislation and shall remain liable to the Data Discloser for the acts and/or omissions of the Processor.

9.3 The Data Receiver may not transfer Shared Personal Data to a third party located outside the UK unless it:

a) Complies with the provisions of the Data Protection Legislation in the event the third party is a joint controller; and

b) Ensures that (i) the transfer is to a country approved under the applicable Data Protection Legislation as providing adequate protection; or (ii) there are appropriate safeguards or binding corporate rules in place pursuant to the applicable Data Protection Legislation; or (iii) the transferee otherwise complies with the Data Receiver's obligations under the applicable Data Protection Legislation by providing an adequate level of protection to any Shared Personal Data that is transferred; or (iv) one of the derogations for specific situations in the applicable Data Protection Legislation applies to the transfer.

10. SECURITY

10.1 The Data Discloser shall only provide the Shared Personal Data to the Data Receiver by using secure methods as set out below:

[Insert any agreed methods of sharing personal data]

10.2 The Parties undertake to have in place throughout this Agreement appropriate technical and organisational security measures to:

a) Prevent:

- Unauthorised or unlawful processing of the Shared Personal Data; and
- The accidental loss or destruction of, or damage to, the Shared Personal Data.

b) Ensure a level of security appropriate to:

- The harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage; and
- the nature of the Shared Personal Data to be protected.

[Such measures shall include: [**Insert Details of any agreed security measures**]]

10.3 It is the responsibility of each Party to ensure that its staff members are appropriately trained to handle and process the Shared Personal Data in accordance with applicable Data Protection Legislation and have entered into confidentiality agreements relating to the Processing of Personal Data.

10.4 The level, content and regularity of training referred to in Clause 10.3 shall be proportionate to the staff members' role, responsibility and frequency with respect to their handling and Processing of the Shared Personal Data.

11. PERSONAL DATA BREACHES AND REPORTING PROCEDURES

11.1 The Parties shall each comply with its obligation to report a Personal Data Breach to the Information Commission and (where applicable) Data Subjects under the Data Protection Legislation and shall each inform the other Party of any Personal Data Breach irrespective of whether there is a requirement to notify the Information Commission or Data Subject(s).

11.2 The Parties agree to provide reasonable assistance as is necessary to each other to facilitate the handling of any Personal Data Breach in an expeditious and compliant manner.

12. REVIEW AND TERMINATION OF THIS AGREEMENT

12.1 The Parties shall review the effectiveness of this data sharing initiative every **[number]** months and on the addition and removal of a Party, having consideration to the aims and purposes set out in Clause 2.2 and Clause 2.3. The Parties shall continue, amend or terminate this Agreement depending on the outcome of this review.

12.2 [Either Party may terminate this Agreement with the other Party by serving not less than 30 days written notice to the other Party. In such case this Agreement shall terminate on expiry of that notice].

12.3 [The Data Discloser may terminate this Agreement immediately upon written notice to the Data Discloser in the event the Data Discloser finds (acting reasonably) that the Data Receiver is no longer acting in compliance with its obligations under this Agreement].

13. RESOLUTION OF DISPUTES WITH DATA SUBJECTS AND THE INFORMATION COMMISSION

13.1 In the event of a dispute, complaint or claim brought by a Data Subject or the Information Commission concerning the processing of Shared Personal Data against either or both Parties, the Parties will inform each other in writing about any such disputes, complaints or claims, and will cooperate with a view to settling them amicably in a timely fashion in line with any timescales contained in the Data Protection Legislation and/or any timescales set out by the Information Commission.

13.2 Each Party shall abide by a decision of a competent court in the UK or of the Information Commission.

14. WARRANTIES

14.1 Each Party warrants and undertakes that it will:

a) Process the Shared Personal Data in compliance with all applicable laws, enactments, regulations, orders, standards and other similar instruments that apply to its Personal Data processing operations.

b) Respond within a reasonable time and as far as reasonably possible to enquiries from the Information Commission in relation to the Shared Personal Data.

c) Respond to Subject Rights Requests and complaints made by Data Subjects concerning the processing of the Shared Personal Data in accordance with the Data Protection Legislation, including where necessary (i) advising the other Party of any step(s) it should reasonably take in this regard; and (ii) where the legitimate ground relied upon is a Data Subject's consent, the timely operation of an effective procedure if such consent is withdrawn.

d) Where applicable, maintain registration and/or pay the appropriate fees with the Information Commission to process all Shared Personal Data for the Agreed Purpose.

e) Take all appropriate steps to ensure compliance with the security measures set out in Clause 10 above.

14.2 The Data Discloser warrants and undertakes that it is entitled to provide the Shared Personal Data to the Data Receiver and it will take reasonable endeavours to ensure that the Shared Personal Data is accurate.

14.3 The Data Receiver warrants and undertakes that it will not disclose or transfer the Shared Personal Data to a third party Controller located outside the UK unless it complies with the obligations set out in Clause 9.3 above.

14.4 Except as expressly stated in this Agreement, all warranties, conditions and terms, whether express or implied by statute, common law or otherwise are hereby excluded to the greatest extent permitted by law.

15. INDEMNITY

15.1 [The Data Discloser and Data Receiver undertake to indemnify each other and hold each other harmless from any cost, charge, damages, expense or loss which they cause each other as a result of their breach of any of the provisions of this Agreement, except to the extent that any such liability is excluded under Clause 17.2.

15.2 [Indemnification hereunder is contingent upon:

a) The Party(ies) to be indemnified (the indemnified Party(ies)) promptly notifying the other Party(ies) (the indemnifying Party(ies)) of a claim,

b) The indemnifying Party(ies) having sole control of the defence and settlement of any such claim, and

c) The indemnified Party(ies) providing reasonable co-operation and assistance to the indemnifying Party(ies) in defence of such claim.] OR

[NOT USED]

16. ALLOCATION OF COST

16.1. Each Party shall perform its obligations under this Agreement at its own cost.

17. LIMITATION OF LIABILITY

17.1 Nothing in this Agreement limits any liability for:

a) Fraud or fraudulent misrepresentation;

b) Death or personal injury caused by negligence;

c) A breach of any obligations implied by section 12 of the Sale of Goods Act 1979; or

d) Any liability that cannot legally be limited.

17.2 Subject to Clause 17.1, neither Party shall in any circumstances be liable whether in contract, delict (including for negligence and breach of statutory duty howsoever arising), misrepresentation (whether innocent or negligent), restitution or otherwise, for:

a) Any loss (whether direct or indirect) of profits, business, business opportunities, revenue, turnover, reputation or goodwill;

b) Loss (whether direct or indirect) of anticipated savings or wasted expenditure (including management time); or

c) Any loss or liability (whether direct or indirect) under or in relation to any other contract.

17.3 Clause 17.2 shall not prevent claims, for:

a) Direct financial loss that are not excluded under any of the categories set out in Clause 17.2(a); or

b) Tangible property or physical damage.

18. THIRD PARTY RIGHTS

18.1 Unless it expressly states otherwise, the Contract does not give rise to any rights under the Contract (Third Party Rights) (Scotland) Act 2017 for any third party to enforce or otherwise invoke any term of the Contract.

19. VARIATION

19.1 No variation of this Agreement shall be effective unless it is in writing and signed by the Parties.

20. WAIVER

20.1 A waiver of any right or remedy is only effective if given in writing and shall not be deemed a waiver of any subsequent right or remedy.

20.2 A delay or failure to exercise, or the single or partial exercise of, any right or remedy does not waive that or any other right or remedy, nor does it prevent or restrict the further exercise of that or any other right or remedy.

21. SEVERANCE

21.1 If any provision or part-provision of this Agreement is or becomes invalid, illegal or unenforceable, it shall be deemed deleted, but that shall not affect the validity and enforceability of the rest of this Agreement.

21.2 If any provision or part-provision of this Agreement is deemed deleted under Clause 21.1, the Parties shall negotiate in good faith to agree a replacement provision that, to the greatest extent possible, achieves the intended commercial result of the original provision.

22. NO PARTNERSHIP OR AGENCY

22.1 Nothing in this Agreement is intended to, or shall be deemed to, establish any partnership or joint venture between any of the Parties, constitute any Party the agent of another Party, or authorise any Party to make or enter into any commitments for or on behalf of any other Party.

22.2 Each Party confirms it is acting on its own behalf and not for the benefit of any other person.

23. ENTIRE AGREEMENT

23.1 This Agreement constitutes the entire agreement between the Parties and supersedes and extinguishes all previous and contemporaneous agreements, promises, assurances and understandings between them, whether written or oral, relating to its subject matter.

23.2 Each Party acknowledges that in entering into this Agreement it does not rely on any statement, representation, assurance or warranty (whether made innocently or negligently) that is not set out in this Agreement.

23.3 Each Party agrees that it shall have no claim for innocent or negligent misrepresentation based on any statement in this Agreement.

24. FURTHER ASSURANCE

24.1 Each Party shall, and shall use all reasonable endeavours to procure that any necessary third Party shall, promptly execute and deliver such documents and perform such acts as may reasonably be required for the purpose of giving full effect to this Agreement.

25. RIGHTS AND REMEDIES

25.1 The rights and remedies provided under this Agreement are in addition to, and not exclusive of, any rights or remedies provided by law.

26. NOTICE

26.1 A notice given to a Party under or in connection with this Agreement shall be in writing and addressed to the SPoCs.

26.2 This Clause 26.2 sets out the delivery methods for sending a notice to a Party under this Agreement and, for each delivery method, the date and time when the notice is deemed to have been received:

a) If delivered by hand, at the time the notice is left at the address;

b) If sent by pre-paid recorded first-class post or other next working day recorded delivery service, at 9.00 am on the second Business Day after posting; or

c) If sent by email, at the time of transmission.

26.3 If deemed receipt under Clause 26.2 would occur outside business hours in the place of receipt, it shall be deferred until business hours resume. In this Clause 26.3, business hours means 9.00am to 5.00pm Monday to Friday on a day that is not a public holiday in the place of receipt.

26.4 This clause does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

27. COUNTERPARTS

27.1 Where executed in counterparts:

a) This Agreement shall not take effect until all of the counterparts have been delivered; and

b) Delivery will take place when the date of delivery is agreed between the Parties after execution of this Agreement as evidenced by the date inserted at the start of this Agreement.

28. GOVERNING LAW AND JURISDICTION

28.1 This Agreement and any dispute or claim (including non-contractual disputes or claims) arising out of or in connection with it or its subject matter or formation shall be governed by and construed in accordance with the law of Scotland.

28.2 Each Party irrevocably agrees that the courts of Scotland shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims), arising out of or in connection with this Agreement or its subject matter or formation.

IN WITNESS WHEREOF this Agreement consisting of this and the preceding [**Insert**] pages is executed as follows and is delivered for the purposes of the Legal Writings (Counterparts and Delivery) (Scotland) Act 2015 on the date set out on page 1 of this Agreement:

Data Discloser

Authenticated for and on behalf of

Yoker Housing Association Limited

Acting by

..... [Authorised Signatory]

Data Receiver

[Insert Full Name of Data Receiver]

Acting by

..... [Director]

For the purposes of the Legal Writings (Counterparts and Delivery) (Scotland) Act 2015, this Agreement is delivered on _____

DATA PROTECTION ADDENDUM

between

Yoker Housing Association Limited, a Scottish Charity (Scottish Charity Number SC036604), a registered society under the Co-operative and Community Benefit Societies Act 2014 with Registered Number 1998RS and having their Registered Office at 2310 Dumbarton Road, Yoker, Glasgow, G14 0JS (the "Association");

and

[[**Full Company Name**] incorporated and registered [**Scotland**] with company number [**Number**] whose registered office is at [**Registered Office Address**] (the "**Processor**")
(each a "**Party**" and together the "**Parties**")

WHEREAS

(a) The Association and the Processor have entered in to an agreement on [**Insert Date [or] [on or about the date of this Data Protection Addendum**] concerning **[Insert Detail]** (hereinafter the "**Principal Agreement**");

(b) This Data Protection Addendum forms part of the Principal Agreement;

(c) This Data Protection Addendum sets out additional terms, requirements and conditions on which the Processor shall process personal data on behalf of the Association when [**performing services**] under the Principal Agreement.

1. DEFINITIONS AND INTERPRETATION

The following definitions and rules of interpretation apply in this Agreement.

1.1 Definitions:

Business Purposes: [the services to be provided by the Processor to the Association as described in the Principal Agreement].

Commission:

a) Until such times as section 118 of the Data (Use and Access) Act 2025 comes into force, the Information Commissioner (see Article 4(A3), UK GDPR and section 114, Data Protection Act 2018); or

b) From the commencement of section 118 of Data (Use and Access) Act 2025 the Information Commission (see section 117 of such Act and section 114A of the Data Protection Act 2018 (when in force)); or

c) Any successor bodies.

Data Protection Legislation: all applicable data protection and privacy legislation in force from time to time in the UK including without limitation the UK GDPR; the Data Protection Act 2018 (and regulations made thereunder) (DPA 2018); the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended; and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications).

Personal Data: means any information relating to an identified or identifiable living individual that is processed by the Processor on behalf of the Association as a result of, or in connection with, the provision of the [services under the Principal Agreement]; an identifiable living individual is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

Processor's Personnel: has the meaning given in Clause 4.1.

UK GDPR: has the meaning set out in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018.

Controller, **Processor**, **Data Subject**, **Personal Data Breach** and **Processing**: have the meanings given in the Data Protection Legislation.

1.2 This Agreement is subject to the terms of the Principal Agreement and is incorporated into the Principal Agreement. Interpretations and defined terms set forth in the Principal Agreement apply to the interpretation of this Agreement.

1.3 The Schedule form part of this Agreement and will have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the Schedule.

1.4 A reference to writing or written excludes fax but not email.

1.5 In the case of conflict or ambiguity between:

1.5.1 Any provision contained in the body of this Agreement and any provision contained in the Schedule, the provision in the body of this Agreement will prevail;

1.5.2 The terms of any accompanying invoice or other documents annexed to this Agreement and any provision contained in the Schedule, the provision contained in the Schedule will prevail; and

1.5.3 Any of the provisions of this Agreement and the provisions of the Principal Agreement, the provisions of this Agreement will prevail.

1.6 A reference to a legislation or legislative provision shall include all subordinate legislation made from time to time under that legislation or legislative provision.

2. PERSONAL DATA TYPES AND PROCESSING PURPOSES

The Association and the Processor agree and acknowledge that for the purpose of the Data Protection Legislation:

2.1 The Association is the Controller and the Processor is the Processor.

2.2 The Association retains control of the Personal Data and remains responsible for its compliance obligations under the Data Protection Legislation, including but not limited to, providing any required notices and obtaining any required consents, and for the written processing instructions it gives to the Processor.

2.3 Part 1 of the Schedule describes the subject matter, duration, nature and purpose of the processing and the Personal Data categories and Data Subject types in respect of which the Processor may process the Personal Data to fulfil the Business Purposes.

3. PROCESSOR'S OBLIGATIONS

3.1 The Processor will only process the Personal Data to the extent, and in such a manner, as is necessary for the Business Purposes in accordance with the Association's written instructions. The Processor will not process the Personal Data for any other purpose or in a way that does not comply with this Agreement or the Data Protection Legislation, except if the Processor is required to otherwise process personal data in accordance with any law which the Processor is subject. In such case the Processor shall, to the extent permitted by law, inform the Association of that requirement before such processing.

3.2 The Processor must promptly notify the Association if, in its opinion, the Association's instructions do not comply with the Data Protection Legislation.

3.3 The Processor must comply promptly with any of the Association's written instructions requiring the Processor to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.

3.4 The Processor shall, insofar as permitted by law, will maintain the confidentiality of the Personal Data.

3.5 The Processor will reasonably assist the Association, at no additional cost to the Association, with meeting the Association's compliance obligations under the Data Protection Legislation, taking into account the nature of the Processor's processing and the information available to the Processor, including in relation to Data Subject rights, complaints submitted by Data Subjects, data protection impact assessments and reporting to and consulting with the Commission under the Data Protection Legislation.

3.6 The Processor must notify the Association promptly of any changes to the Data Protection Legislation that may reasonably be interpreted as adversely affecting the Processor's performance of the Principal Agreement or this Agreement.

3.7 The Processor shall comply with all applicable requirements of the Data Protection Legislation. This clause 3.7 is in addition to, and does not relieve, remove or replace, the Processor's obligations or rights under the Data Protection Legislation.

4. PROCESSOR'S EMPLOYEES

4.1 The Processor will ensure that all of its employees, agents, advisors and consultants who have access to the Personal Data ("**Processor's Personnel**"):

4.1.1 Are informed of the confidential nature of the Personal Data and are bound by written confidentiality obligations and use restrictions in respect of the Personal Data;

4.1.2 Have undertaken training on the Data Protection Legislation and how it relates to their handling of the Personal Data and how it applies to their particular duties; and

4.1.3 Are aware both of the Processor's duties and their personal duties and obligations under the Data Protection Legislation and this Agreement.

4.2 The Processor will:

4.2.1 Take reasonable steps to ensure the reliability, integrity and trustworthiness of all of the Processor's Personnel with access to the Personal Data; and

4.2.2 Limit such access to the Personal Data to those persons who need to have access to it in the performance of their duties.

5 SECURITY

5.1 The Processor must at all times implement appropriate technical and organisational measures against accidental, unauthorised or unlawful processing, access, copying, modification, reproduction, display or distribution of the Personal Data, and against accidental or unlawful loss, destruction, alteration, disclosure or damage of Personal Data [including, but not limited to, the security measures set out in Part 2 of the Schedule].

5.2 The Processor must implement such measures to ensure a level of security appropriate to the risk involved, including as appropriate:

5.2.1 The pseudonymisation and encryption of personal data;

5.2.2 The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

5.2.3 The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and

5.2.4 A process for regularly testing, assessing and evaluating the effectiveness of the security measures.

6. PERSONAL DATA BREACH

6.1 The Processor will immediately and in any event without undue delay notify the Association in writing if it becomes aware of any Personal Data Breach.

6.2 Where the Processor becomes aware of any Personal Data Breach it will, without undue delay, provide the Association with the following written information:

6.2.1 Description of the Personal Data Breach, including the categories of in-scope Personal Data and approximate number of both Data Subjects and the Personal Data records concerned;

6.2.2 the likely consequences of the Personal Data Breach; and

6.2.3 a description of the measures taken or proposed to be taken to address the Personal Data Breach, including measures to mitigate its possible adverse effects.

6.3 Immediately following any Personal Data Breach the Parties will co-ordinate with each other to investigate the matter. Further, the Processor will reasonably co-operate with the Association at no additional cost to the Association, in the Association's handling of the matter.

6.4 The Processor will not inform any third-party of any accidental, unauthorised or unlawful processing of all or part of the Personal Data and/or a Personal Data Breach without first obtaining the Association's written consent, except when required to do so by law.

7. TRANSFERS OF PERSONAL DATA

7.1 The Processor (and any subcontractor) must not transfer or otherwise process the Personal Data outside the UK unless the prior written consent of the Association has been obtained and the following conditions are fulfilled:

7.1.1 The Association or the Processor has provided appropriate safeguards in relation to the transfer;

7.1.2 The data subject has enforceable rights and effective legal remedies;

7.1.3 The Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred; and

7.1.4 The Processor complies with reasonable instructions notified to it in advance by the Association with respect to the processing of the Personal Data.

8. SUBCONTRACTORS

8.1 The Processor may only authorise a third-party (subcontractor) to process the Personal Data if:

8.1.1 The Association [provides written consent prior to the appointment of each subcontractor] OR [is provided with an opportunity to object to the appointment of each subcontractor within [number] working days after the Processor supplies the Association with full details in writing regarding such subcontractor];

8.1.2 The Processor enters into a written contract with the subcontractor that contains terms substantially the same as those set out in this Agreement, in particular, in relation to requiring appropriate technical and organisational data security measures, and, upon the Association's written request, provides the Association with copies of the relevant excerpts from such contracts;

8.1.3 The Processor maintains control over all of the Personal Data it entrusts to the subcontractor; and

8.1.4 The subcontractor's contract terminates automatically on termination of this Agreement for any reason.

8.2 [Those subcontractors approved as at the commencement of this Agreement are as set out in Part 1 of the Schedule. The Processor must list all approved subcontractors in Part 1 of the Schedule and include any subcontractor's name and location and the contact information for the person responsible for privacy and data protection compliance.] OR [NOT USED]

8.3 Where the subcontractor fails to fulfil its obligations under the written agreement with the Processor which contains terms substantially the same as those set out in this Agreement, the Processor remains fully liable to the Association for the subcontractor's performance of its agreement obligations.

8.4 The Parties agree that the Processor will be deemed by them to control legally any Personal Data controlled practically by or in the possession of its subcontractors.

9. COMPLAINTS, DATA SUBJECT REQUESTS AND THIRD-PARTY RIGHTS

9.1 The Processor must, at no additional cost to the Association, take such technical and organisational measures as may be appropriate, and promptly provide such information to the Association as the Association may reasonably require, to enable the Association to comply with:

9.1.1 The rights of Data Subjects under the Data Protection Legislation, including, but not limited to, subject access rights, the rights to rectify, port and erase personal data, object to the processing, the right to submit a complaint to a controller and automated processing of personal data, and restrict the processing of personal data; and

9.1.2 Information or assessment notices served on the Association by the Commission under the Data Protection Legislation.

9.2 The Processor must notify the Association immediately in writing if it receives any complaint, notice or communication that relates directly or indirectly to the processing of the Personal Data or to either party's compliance with the Data Protection Legislation.

9.3 The Processor must notify the Association within 24 hours if it receives a request from a Data Subject for access to their Personal Data or to exercise any of their other rights under the Data Protection Legislation.

9.4 The Processor will give the Association, at no additional cost to the Association, its full co-operation and assistance in responding to any complaint, notice, communication or Data Subject request or request.

9.5 The Processor must not disclose the Personal Data to any Data Subject or to a third-party other than in accordance with the Association's written instructions, or as required by law.

10. TERM AND TERMINATION

10.1 This Agreement will remain in full force and effect so long as:

10.1.1 the Principal Agreement remains in effect; or

10.1.2 the Processor retains any of the Personal Data related to the Principal Agreement in its possession or control.

10.2 Any provision of this Agreement that expressly or by implication should come into or continue in force on or after termination of the Principal Agreement in order to protect the Personal Data will remain in full force and effect.

10.3 The Processor's failure to comply with the terms of this Agreement is a material breach of the Principal Agreement. In such event, the Association may terminate [the Principal Agreement OR any part of the Principal Agreement involving the processing of the Personal Data] effective immediately on written notice to the Processor without further liability or obligation of the Association.

11. DATA RETURN AND DESTRUCTION

11.1 At the Association's request, the Processor will give the Association, or a third-party nominated in writing by the Association, a copy of or access to all or part of the Personal Data in its possession or control in the format and on the media reasonably specified by the Association.

11.2 On termination of the Principal Agreement for any reason or expiry of its term, the Processor will securely delete or destroy or, if directed in writing by the Association, return and not retain, all or any of the Personal Data related to this Agreement in its possession or control.

11.3 If any law, regulation, or government or regulatory body requires the Processor to retain any documents, materials or Personal Data that the Processor would otherwise be required to return or destroy, it will notify the Association in writing of that retention requirement, giving details of the documents, materials or Personal Data that it must retain, the legal basis for such retention, and establishing a specific timeline for deletion or destruction once the retention requirement ends.

11.4 The Processor will certify in writing to the Association that it has deleted or destroyed the Personal Data within 5 days after it completes the deletion or destruction.

12. RECORDS AND AUDIT

12.1 the Processor will keep detailed, accurate and up-to-date written records regarding any processing of the Personal Data, including but not limited to, the access, control and security of the Personal Data, approved subcontractors, the processing purposes, categories of processing, and a general description of the technical and organisational security measures.

12.2 The Processor will ensure that the Records are sufficient to enable the Association to verify the Processor's compliance with its obligations under this Agreement and the Data Protection Legislation and the Processor will provide the Association with copies of the Records upon request.

12.3 The Processor will allow for audits of the Records by the Association and/or any person appointed on their behalf.

13. WARRANTIES

13.1 The Processor warrants and represents that:

13.1.1 The Processor's Personnel and any other person or persons accessing the Personal Data on its behalf are reliable and trustworthy and have received the required training on the Data Protection Legislation;

13.1.2 it and anyone operating on its behalf will process the Personal Data in compliance with the Data Protection Legislation and other laws, enactments, regulations, orders, standards and other similar instruments;

13.1.3 it has no reason to believe that the Data Protection Legislation prevents it from providing any of the Master Agreement's contracted services; and

13.1.4 considering the current technology environment and implementation costs, it will take appropriate technical and organisational measures to prevent the accidental, unauthorised or unlawful processing of Personal Data and the loss or damage to, the Personal Data, and ensure a level of security appropriate to the harm that might result from such accidental, unauthorised or unlawful processing and loss or damage and the nature of the Personal Data.

13.2 The Association warrants and represents that the Processor's expected use of the Personal Data for the Business Purposes and as specifically instructed by the Association will comply with the Data Protection Legislation.

14. INDEMNIFICATION

14.1 [The Processor agrees to indemnify, keep indemnified and defend at its own expense the Association against all costs, claims, damages or expenses incurred by the Association or for which the Association may become liable due to any failure by the Processor or its employees, subcontractors or agents to comply with any of its obligations under this Agreement and/or the Data Protection Legislation.

14.2 Any limitation of liability set forth in the Principal Agreement will not apply to this Agreement's indemnity or reimbursement obligations.] OR [NOT USED]

15. COUNTERPARTS

15.1 Where executed in counterparts:

15.1.1 This Agreement shall not take effect until all of the counterparts have been delivered; and

15.1.2 Delivery will take place when the date of delivery is agreed between the Parties after execution of this Agreement as evidenced by the date inserted at the start of this Agreement.

16. GOVERNING LAW AND JURISDICTION

16.1 The Parties hereby submit to the choice of jurisdiction stipulated in the Principal Agreement 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

16.2 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.

IN WITNESS WHEREOF this Agreement consisting of this and the preceding [**Insert**] pages together with the Schedule appended hereto is executed as follows and is delivered for the purposes of the Legal Writings (Counterparts and Delivery) (Scotland) Act 2015 on the date set out on page 1 of this Agreement:

Controller

Authenticated for and on behalf of

Yoker Housing Association Limited

Acting by

..... [Authorised Signatory]

Processor

[INSERT FULL NAME OF PROCESSOR]

Acting by

..... [Director]

THIS IS THE SCHEDULE REFERRED TO IN THE FOREGOING DATA PROTECTION ADDENDUM AMONG YOKER HOUSING ASSOCIATION LIMITED AS CONTROLLER AND [Insert Full Name of Processor] AS PROCESSOR

PART 1

PERSONAL DATA PROCESSING PURPOSES AND DETAILS

Subject matter of processing: [Short description, for example name of the service or description of the Principal Agreement]

Duration of Processing: [Periods for which the services are being provided]

Nature of Processing: [Description of the type of processing such as data collection, storage, sharing and so on]

Business Purposes: [Description of the processing purpose(s) – for example processing for HR purposes, recruitment, direct marketing and so on]

Personal Data Categories: [Set out types of personal data such as names, contact details, pay details, images and so on]

Data Subject Types: [Set out categories of data subjects such as employees, customers, students and so on]

Approved Subcontractors:

- [List all approved subcontractors.]

PART 2

SECURITY MEASURES

[Insert]

DEFINITIONS

Controller, Processor, Data Subject, Personal Data, Personal Data Breach, processing and appropriate technical and organisational measures: as defined in the Data Protection Legislation.

Data Protection Legislation: all applicable data protection and privacy legislation in force from time to time in the UK including the UK GDPR; the Data Protection Act 2018 (DPA 2018) (and regulations made thereunder) and the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426) as amended and all other legislation and regulatory requirements in force from time to time which apply to a Party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications);

Domestic Law: the law of the United Kingdom or a part of the United Kingdom.

UK GDPR: has the meaning set out in section 3(10) (as supplemented by section 205(4)) of the Data Protection Act 2018.

1. DATA PROTECTION

1.1 Both Parties will comply with all applicable requirements of the Data Protection Legislation. This clause [1] is in addition to, and does not relieve, remove or replace, a Party's obligations or rights under the Data Protection Legislation.

1.2 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Customer is the Controller and the Provider is the Processor. Schedule [Number] sets out the scope, nature and purpose of processing by the Provider, the duration of the processing and the types of Personal Data and categories of Data Subject.

1.3 Without prejudice to the generality of Clause [1.1], the Customer will ensure that it has all necessary appropriate consents and notices in place to enable lawful transfer of the Personal Data to the Provider [and/or lawful collection of the Personal Data by the Provider on behalf of the Customer] for the duration and purposes of this agreement.

1.4 Without prejudice to the generality of Clause 1.1, the Provider shall, in relation to any Personal Data processed in connection with the performance by the Provider of its obligations under this agreement:

1.4.1 Process that Personal Data only on the documented written instructions of the Customer [which are set out in [Schedule [NUMBER] OR [DOCUMENT] OR [this agreement] unless the Provider is required by Domestic Law to otherwise process that Personal Data. Where the Provider is relying on Domestic Law as the basis for processing Personal Data, the Provider shall promptly notify the Customer of this before performing the processing required by the Domestic Law unless the Domestic Law prohibits the Provider from so notifying the Customer;

1.4.2 Ensure that it has in place appropriate technical and organisational measures, reviewed and approved by the Customer, to protect against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, having regard to the state of technological development and the cost of implementing any measures (those measures may include, where appropriate, pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of its systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of the technical and organisational measures adopted by it);

1.4.3 Ensure that all personnel who have access to and/or process Personal Data are obliged to keep the Personal Data confidential; and

1.4.4 Not transfer any Personal Data outside of the UK unless the prior written consent of the Customer has been obtained and the following conditions are fulfilled:

a) The Customer or the Provider has provided appropriate safeguards in relation to the transfer;

b) The data subject has enforceable rights and effective legal remedies;

c) The Provider complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any Personal Data that is transferred; and

d) The Provider complies with reasonable instructions notified to it in advance by the Customer with respect to the processing of the Personal Data.

1.4.5 Assist the Customer, at the Customer's cost, in responding to any request from a Data Subject and in ensuring compliance with its obligations under the Data Protection Legislation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;

1.4.6 Notify the Customer without undue delay on becoming aware of a Personal Data Breach;

1.4.7 At the written direction of the Customer, delete or return Personal Data and copies thereof to the Customer on termination of the agreement unless required by Domestic Law to store the Personal Data; and

1.4.8 Maintain complete and accurate records and information to demonstrate its compliance with this clause [1] and allow for audits by the Customer or the Customer's designated auditor and immediately inform the Customer if, in the opinion of the Provider, an instruction infringes the Data Protection Legislation.

1.5 The Provider may only authorise a third-party (subcontractor) to process the Personal Data if:

1.5.1 The Customer [provides written consent prior to the appointment of each subcontractor] OR [is provided with an opportunity to object to the appointment of each subcontractor within [NUMBER] working days after the Provider supplies the Customer with full details in writing regarding such subcontractor];

1.5.2 The Provider enters into a written contract with the subcontractor that contains terms substantially the same as those set out in this agreement, in particular, in relation to requiring appropriate technical and organisational data security measures, and, upon the Customer's written request, provides the Customer with copies of the relevant excerpts from such contracts;

1.5.3 The Provider maintains control over all of the Personal Data it entrusts to the subcontractor; and

1.5.4 The subcontractor’s processing of the Personal Data ceases on termination of this agreement for any reason.

SCHEDULE [Insert]

PERSONAL DATA PROCESSING PURPOSES AND DETAILS

Subject matter of processing: [Short description, for example name of the service or description of the master agreement]

Duration of Processing: [Periods for which the services are being provided]

Nature of Processing: [Description of the type of processing such as data collection, storage, sharing and so on]

Business Purposes: [Description of the processing purpose(s) – for example processing for HR purposes, recruitment, direct marketing and so on]

Personal Data Categories: [Set out types of personal data such as names, contact details, pay details, images and so on]

Data Subject Types: [Set out categories of data subjects such as employees, customers, students and so on]

Authorised Persons: [Insert details of employees/others authorised to give written instructions]

Introduction

Yoker Housing Association Limited (the Association) is committed to ensuring the secure and safe management of data held by the Association in relation to customers, staff and other individuals.

As part of this, the Association wishes to ensure that if an individual complains to us about how we process their personal data, we have a robust process in place for handling this complaint and addressing any valid concerns.

About this document

This process sets out how individuals (Data Subjects) can raise complaints about how the Association collects, uses, stores, shares, or otherwise processes their personal data. It ensures compliance with the UK GDPR, the Data Protection Act 2018 and other data protection laws.

This process applies to all complaints relating to:

- Alleged breaches of UK data protection law;
- Handling of personal information (accuracy, retention, security, lawful basis, etc.); or
- Responses to data subject rights requests (e.g. subject access requests).

In this process, a complaint means "any expression of dissatisfaction by a data subject about how their personal data has been processed by the Association".

If your complaint includes other service delivery issues or issues which are covered by other legislation (for example a request for review under Freedom of Information), the Association will handle those aspects of your complaint under our relevant policies or legal requirements.

How to Submit a Complaint

How to submit a complaint

Individuals can submit a complaint by:

- Using the complaints form that can be downloaded from our website at https://www.yokerha.org.uk/data/Data_Protection_Complaints_Form_2026_06_02_10_22_05.pdf or
- By submitting a complaint by post to Data Protection Officer, Yoker Housing Association Limited, 2310 Dumbarton Road, Yoker, Glasgow, G14 0JS.

What information should your complaint include?

The Association's complaint form sets out the information required, but generally, we will require the following information:

- Your name and contact details
- A description of the concern
- Any relevant dates and any supporting evidence
- What outcome you are seeking

The Association may need to ask you to provide further information in the course of reviewing your complaint.

Verifying your identity

We may need to verify your identity to progress your complaint. What verification we require will depend on our relationship with you and will be taken on a case-by-case basis. The Association will be reasonable and proportionate about the verification needed.

Making a complaint on another person's behalf

If you are making a complaint on the data subject's behalf (e.g. you are their family member or solicitor), the Association will require satisfactory of evidence of your authority to act on the data subject's behalf in respect of the complaint. If you do not provide this, the Association cannot investigate your complaint.

Acknowledgement of Complaints

The Association will acknowledge receipt of a complaint as quickly as possible, any in any event, within 30 calendar days of receipt. This acknowledgement will:

- Confirm receipt of the complaint;
- Provide a reference number for the complaint; and
- Outline the Association's next steps and expected timescales for dealing with the complaint.

Handling Complaints

Upon receipt of a complaint, the Association will:

- Assign an appropriate individual (e.g. the Association's Data Protection Officer or other lead) to manage the complaint;
- Conduct an initial assessment of the complaint to determine: if it is within scope and if further information is needed to investigate (e.g. verification of your identity); and
- Take appropriate steps to investigate and respond without undue delay. This includes making enquiries into the matter and reviewing relevant records and processes.

During the investigation the Association will keep you informed on the progress of the complaint.

Outcome of the Complaint

Once the Association has completed the investigation it will provide you with the outcome of the complaint. This will normally be done in writing.

The outcome will include:

- A summary of the issues investigated;
- Conclusions reached;
- Any corrective action taken (if applicable); and
- Information about further escalation options.

External Escalation

If you are unhappy with the outcome of your complaint you may refer your complaint to the Information Commissioner's Office (ICO).

The ICO is an independent body whose role is to uphold data protection law in the UK. The ICO provides information on their website about how to make a complaint and this can be accessed by visiting:

www.ico.org.uk/make-a-complaint/data-protection-complaints/

If you cannot access the internet please advise the Association so that we can provide you with the ICO's contact details.

You may also seek judicial remedy for certain data protection issues.

Record Keeping and Review

The Association will review the outcome of complaints to identify any areas where our performance can be improved.

Publication and Accessibility

We will publish this process on our website and in accordance with our obligations under the Freedom of Information (Scotland) Act 2002.

We will ensure reasonable adjustments are made to support those who may need assistance accessing this process and making a complaint. If you require any such assistance please contact the Association's Data Protection Officer.

Yoker Housing Association Limited - Data Protection Complaints Form

About this Form

This form is for individuals who wish to submit a complaint about how Yoker Housing Association Limited (the Association) has handled their personal data. This includes concerns about how an individual's personal data has been collected, used, stored, shared, or how the Association has handled a data protection rights request (e.g. a subject access request or erasure request).

You do not have to use this form to make a complaint – you may also contact us by email, post, or telephone. However, using this form will help us investigate your complaint more efficiently.

Section 1 – Your Details

Full Name	
Title:	☐ Mr ☐ Ms ☐ Mrs ☐ Mx ☐ Other
Name:	
Contact Details	
Email Address	
Telephone Number	
Address	
Preferred Method of Contact	☐ Email ☐ Post ☐ Telephone

Note: the Association may require further information to verify your identity. If this is the case we will contact you and let you know what we require.

Section 2 – Are you Complaining on Behalf of Someone Else?

Are you complaining on behalf of another individual? ☐ No ☐ Yes

If yes, please confirm your relationship to the individual: _____

Have you provided written authority from the individual to act on their behalf in connection with the complaint?:

☐ Yes ☐ No

Please note: If you are unable to provide authority we will not be able to investigate the complaint.

Section 3 – Details of your Complaint

What is your complaint about?

(Please describe your concern clearly, including what personal data is involved and what you believe has gone wrong.)

Please provide relevant dates

(For example, when the issue occurred or when you became aware of it.)

Have you contacted us about this issue before? ☐ Yes ☐ No

If yes, please provide details (for example, date, reference number, who you contacted):

Section 4 – Supporting Information

Do you have any documents or evidence you would like us to consider?

☐ No

☐ Yes (please attach copies, not originals)

Section 5 – Outcome Sought

What outcome are you seeking?

(For example, an explanation, apology, or improvement to our processes.)

Section 6 – Declaration

I confirm that the information provided in this form is accurate to the best of my knowledge: ☐ Yes

Date: _____

What Happens Next

- We will acknowledge receipt of your complaint as quickly as possible and, as a minimum, within 30 calendar days.
- We may contact you if we need further information to investigate your complaint.
- Once our investigation is complete, we will provide you with a response explaining our findings and any action taken.
- If you are dissatisfied with our response, you will be informed of your right to escalate the matter to the Information Commissioner's Office (ICO).

Please see our Data Protection Complaints Process, available at https://www.yokerha.org.uk/data-protection-complaints-process/ for more information on how your complaint will be handled.

How your Data will be Used

For information about how your personal will be used please see our Fair Processing Notice which can be accessed online by visiting https://www.yokerha.org.uk/data-protection/

The table below sets out 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 Periods**
Membership Records.	5 years after last contact.
Personal files including training records and notes of disciplinary and grievance hearings.	5 years to cover the time limit for bringing any civil legal action, including contractual claims.
Redundancy details, calculations of payments, refunds, notification to the Secretary of State.	6 years from the date of the redundancy.
Application forms and interview notes.	Minimum 6 months to 1 year from date of interviews. Successful applicants' 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.	At least 3 years after the end of the tax year they relate to.
Income tax, NI returns, correspondence with tax office.	At least 3 years after the end of the tax year they relate to.
Retirement benefits 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.
Statutory Sick Pay records, calculations, certificates, self-certificates.	3 years.
Wages / salary records, expenses, bonuses.	6 years.
Records relating to working time.	3 years from the date they were made.
Accident books and records and reports of accidents.	6 years after the date of the last entry.
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.
Trade Union Agreements.	10 years after ceasing to be effective.
Board Members Documents.	5 years after cessation of membership.
Documents relation to successful tenders.	5 years after end of contract.
Documents relating to unsuccessful form of tender.	5 years after notification.

Applicants for accommodation.	Duration that application remains live
Housing Benefits Notifications.	Duration of tenancy.
Rent Registration Documentation	6 years.
Tenancy files.	6 months after termination of tenancy
Former tenants' files (key information – e.g. tenancy debts, anti-social behaviour, tenancy breaches).	5 years.
Third Party documents (e.g. care plans).	Duration of tenancy.
Records re offenders and ex-offenders (sex offender register).	Duration of tenancy.
Lease documents.	5 years after lease termination.
ASB case files.	5 years / end of legal action.
Board meetings / residents' meetings (e.g. Agendas, notice of meetings etc)	2 years (this does not refer to minutes of meetings as these must be permanently retained)
Minute of factoring meetings.	Duration of appointment.