Policy Title: **Data Protection Policy**

Policy Manual Section: **Governance**

Date Approved by Management Committee: 31 May 2018

Next Review Date: **May 2021**

This document will be made available in different languages and formats on request, including Braille and audio formats.

ENGLISH This information is available on request in other languages, in large print, in Braille and on audio format. If you or anyone you know would like this information in one of these formats please contact Cadder HA on **0141 945 3282**

POLISH Niniejsze informacje dostępne są na żądanie w innych wersjach językowych, dużym drukiem, językiem Braille'a oraz w formacie audio. Aby otrzymać powyższe informacje w jednym z wymienionych formatów, proszę skontaktować się z Zespołem ds. Cadder HA pod numerem telefonu **0141 945 3282**

FRENCH Ces informations sont disponibles sur demande dans d'autres langues, en gros caractères, en braille et en format audio. Si vous souhaitez obtenir ces informations dans l'un de ces formats, veuillez contacter Cadder HA au **0141 945 3282.**

ARABIC بأحرف بطباعة ،أخرى بلغات الطلب تحت متوفرة المعلومة هذه
في ترغب آنت إذا .صوتي شريط على و برايل بطريقة ، آبيرة
أن الرجاء ،الصيغ هذه من بأي المعلومة هذه على الحصول
للإسكان آلاسكو جمعية سياسة بفريق تتصل Cadder HA
0141 945 الرقم على ***3282***

SOMALI Warbixintaan waxaa, haddii la dalbado lagu heli karaa luuqaddo kale, daabacaad weyn, Farta ay dadka indhaha la' akhriyaan (Braille) iyo qaab cajaladdo maqal ah. Haddii aad doonayso inaad warbixintan ku hesho mid ka mid ah qaababkaas, fadlan kala xidhiidh Kooxda Xeerarka ee Cadder HA telefoonka ***0141 945 3282***

Farsi این مطالب را می توانید به زبان های دیگر، به شکل چاپ با حروف درشت یا
حروف بریل (برای نابینایان) و بر روی نوار صوتی درخواست نمایید. در صورتی آه
مایل به دریافت این مطالب به یکی از شکل های فوق هستید لطفاً با دفت Cadder HA تماس
تلفن شماره .آنید حاصل ***0141 945 3282***

RUSSIAN Данная информация может быть
предоставлена по требованию
на других языках, крупным шрифтом, шрифтом Брайля и в аудиозаписи.
Если вы хотите получить данную
информацию в одном из этих
форматов, обратитесь в Cadder HA по телефону ***0141 945 3282***

Contents

Data Protection Policy

1.0 Introduction

1.1 Cadder Housing Association (the Association) is fully committed to compliance with the requirements of the General Data Protection Regulations (GDPR), which came into force on 25th May 2018. The Association will therefore follow procedures that aim to ensure that all employees, Committee members, contractors, agents, consultants, partners or other persons involved in the work of the Association and who have access to any personal data held by or on behalf of the Association, are fully aware of and abide by their duties and responsibilities under GDPR.

1.2 The Data Protection Policy should be read in conjunction with the Privacy Policy, which details the main requirements for processing personal data.

2.0 Statement of policy

2.1 In order to operate efficiently, the Association has to collect and use information about people with whom we work in order to carry out our business and provide our services. The details of the personal data collected and processed is set out in the Association's Privacy Policy and Privacy Notice.

2.2 The Association regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the Association and the full range of stakeholders in our work. The Association will ensure that it treats personal information lawfully and correctly.

2.3 To this end the Association fully endorses and adheres to the Principles of Data Protection as set out in the GDPR.

3.0 Glossary of Key Terms

3.1 The following is a glossary of key terms in the GDPR, which Committee members, staff and volunteers should be familiar with to execute this policy, they include:

a) Information Commissioner's Office (ICO) – Responsible for enforcing the GDPR and Data Protection legislation. The Association requires to submit an annual notification to the ICO detailing the systems containing data and how the data is used. We are also required to notify the ICO of any changes to the register within 28 days.

b) Data Controller - The organisation that determines the purposes for which and manner in which personal data is used, in our case, the Association.

c) Data Subject – a living individual who is the subject of personal data e.g. tenant, employee, Committee member, suppliers, etc.

d) Personal data

- The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.
- This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people.
- The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.
- Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

e) Sensitive personal data

- The GDPR refers to sensitive personal data as "special categories of personal data" (see Article 9).
- The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.
- Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10).

d) Processing – obtaining, recording or holding data or carrying out any operation on data, including disclosure and destruction.

e) Stakeholder – includes current and former tenants, current and former Committee members, current and former staff including any temporary or work experience appointments, residents, other customers (owners, applicants for housing, and others) consultants, contractors, agents and partners.

4.0 Data Protection Act and Other Associated Legislation and Policy Considerations

4.1 General Data Protection Regulations (GDPR)

GDPR controls how personal data is used by organisations. It sets out the principles on the use or storage of data relating to living people and gives rights to those people whose data has been collected. The key principles of the GDPR are set out in section 5.2 of this policy.

4.2 Human Rights Act 1998

The Human Rights 1998 includes a series of sections that have the effect of codifying the protections in the European Convention of Human Rights into UK law. The Act sets out the fundamental rights and freedoms that individuals in the UK have access to, they include: the right to life; respect for your private and family life, home and correspondence, etc.

The Association will strive to comply fully with the Human Rights Act in our implementation of the GDPR specifically in our use of personal data particularly in relation to protecting the right to respect for private life enjoyed by our stakeholders.

4.3 Freedom of Information (Scotland) Act 2002

The Freedom of Information (Scotland) Act 2002 outlines that public authorities are obliged to publish certain information about their activities; and members of the public are entitled to request information from public authorities.

The provisions of the Freedom of Information (Scotland) Act 2002 do not apply to housing associations. The Association will aim to respond to requests for information in the spirit of legislation and as outlined in our Confidentiality and Openness Policy.

4.4 Housing (Scotland) Act 2001

The Housing (Scotland) Act 2001 introduced the Scottish Secure Tenancy Agreement for all tenants of social landlords in Scotland. It included the tenant's rights to a written agreement and to information on the landlord's policies and procedures. It also outlined the registration and regulation of social landlords and the Scottish Housing Regulator's power to obtain information and any document which is required for the purposes of an inspection.

4.5 Housing (Scotland) Act 2010

The Housing (Scotland) Act 2010 established the Scottish Housing Regulator and the new regulatory framework for social landlords through the Scottish Housing Charter. The Act also outlines the new Regulator's power to obtain information or a document in relation to the activities of the landlord or a body connected to it, including the new annual return on the Scottish Social Housing Charter.

4.6 Other Legislation and Associated Policies

The Association will observe the provisions of the GDPR and this policy in relation to other legislation, good practice guidance and through

other policies. This will be where we require to publish, exchange or process personal information associated with our work and our stakeholders, these include:

a) The Police Act 1997
b) Anti-Social Behaviour, etc. (Scotland) Act 2004
c) Management of Sexual Offenders etc. (Scotland) Act 2005
d) The Criminal Justice (Scotland) Act 2006
e) Equalities Act 2010
f) The Information Commissioner's Data Protection Codes:
    i) Employment Practices
    ii) CCTV
    iii) Data Sharing
g) This policy on data protection should be read in conjunction with policies and governing documents of the Association:
    i) Privacy Policy
    ii) Equality & Diversity Policy
    iii) Allocation Policy
    iv) Unacceptable Actions Policy
    v) EVH Terms and Conditions of Employment
    vi) Anti-Social Behaviour Policy
    vii) Openness and Confidentiality Policy
    viii) Risk Management Policy
    ix) CCTV Policy

5.0 Principles of data protection

5.1 The data protection principles set out the main responsibilities for organisations. Article 5 of the GDPR requires that personal data shall be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

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

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

5.2 Our purpose for holding personal information and a general description of the categories of people and organisations to which we may disclose it, are listed in the Information Commissioner's Data Protection Register, the Association's Privacy Policy and our Privacy Notices.

6.0 Handling of personal/sensitive information

6.1 The Association will, through appropriate management and the use of strict criteria and controls in line with its Privacy Policy and Privacy Notices:-

6.2 The Association will also ensure that:

- There is someone with specific responsibility for data protection in the organisation;
- Everyone within the Association who is managing and handling personal information understands that the Association is legally responsible for following good data protection practice;
- Everyone managing and handling personal information within the Association is appropriately trained to do so;
- Everyone managing and handling personal information within the Association is appropriately supervised;
- Anyone wanting to make enquiries about handling personal information, whether a member of staff, tenant, other customer or stakeholder, etc., knows what to do;
- Queries and complaints about handling personal information are promptly and courteously dealt with in accordance with our Privacy Policy and Complaints Procedure;
- Methods of handling personal information are regularly assessed and evaluated;
- Performance in relation to handling personal information is regularly assessed and evaluated;
- Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

6.3 All Committee members are to be made fully aware of this policy and of the Association's duties and responsibilities under the GDPR.

6.4 All managers and staff within the Association will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular will ensure that:

- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment;
- Access to personal data is only provided on a "need to know" basis to those staff who require access for the purposes of fulfilling the requirements of their role within the Association;
- Appropriate technical measures, including internet security, anti-virus software and firewalls, are installed;
- Personal data held on computers and computer systems is protected by the use of secure passwords, which have forced changes periodically;
- Individual passwords should be such that they are not easily compromised.

Appendix 1 provides further guidance to staff in dealing with personal information. The Association's Document Retention Policy sets out the guidelines for data retention periods.

6.5 All contractors who are users of personal information supplied by the Association will be required to confirm that they will abide by the requirements of the GDPR with regard to information supplied and sign an appropriate Contract Addendum or Data Sharing Agreement as set out in the Privacy Policy.

7.0 Disclosure of Information

7.1 The Association in our role as a housing landlord and employer will need to share information with other organisations, where we do this it will be in line with our Privacy Policy and Privacy Notices.

7.2 The Freedom of Information (Scotland) Act 2002 does not apply to housing associations. However, the Association will aim to abide by the spirit of the legislation and endeavour to respond positively to written requests for information, from whatever source and for whatever reason, unless:

- The request is vexatious;
- The Association has already complied with the request;
- The request is identical or substantially similar to a request previously received from the same individual or organisation;
- The information is covered by an exemption from the requirements set out in the Freedom of Information (Scotland) Act.

7.3 The Association's Confidentiality and Openness Policy gives more details on our approach and associated issues to responding to Freedom of Information requests.

7.4 Further guidance on the information the Association, as a landlord can release, 'How and to Who' is attached as appendix 2.

8.0 Implementation of Policy

8.1 It is essential the Association complies with the GDPR and does not obtain, process and store information for the purposes other than those they have been registered for with the Information Commissioner's Office. To ensure compliance with the GDPR, staff must be aware that this relates to information held on current, former or prospective: tenants; Committee members; customers; residents, applicants for housing, applications for employment, employees, pension administration, payroll and supplier administration. Further details are presented in the Association's Privacy Policy and Privacy Notices.

8.2 This section of the Policy defines the responsibilities for data protection within the Association and should be read in conjunction with the Privacy Policy:

a) The Director has overall responsibility for data protection within the Association.

b) The Association has established a Finance & Corporate Services Department. The Finance & Corporate Services Manager (FCSM) will be designated officer and fulfil the role as Data Controller within the Association and will be responsible for ensuring that the Policy is implemented. The FCSM will have overall responsibility for:

- The provision of data protection training, advice and support for staff within the Association to ensure full compliance with the GDPR;
- For the development of best practice guidelines;
- For carrying out compliance checks to ensure adherence with data protection legislation;
- Managing any complaints in relation to alleged breach of the Data Protection legislation and Policy in the use of personal data; and
- Responding to requests from individuals to access personal information the Association holds on them.

c) Each member of the Senior Staff Team has specific responsibility for personal information held on their staff. Staff will be informed about data protection issues and their rights to access their own personal data through the Employee Privacy Notice, induction process and a staff handbook.

d) Sectional Managers will ensure that personal data processed by their section is included in the Association's data protection register and is kept up to date and complies with the principles of Data Protection as outlined in section 5.2 of this policy.

e) All staff have a responsibility to fully comply with the requirements of the GDPR Act, the Privacy Policy and this policy. When involved in requesting information, staff will provide the individual with a copy of the customer Privacy Notice when first requesting information.

8.3 A copy of this policy will be given to all new members of staff, Committee, contractors, other stakeholders or interested third parties. Existing staff and any relevant stakeholder will be advised of the policy, which will be posted on our server. All staff and stakeholders are to be familiar with and comply with this policy at all times.

9.0 Notification to the Information Commissioner

9.1 The Information Commissioner maintains a public register of data controllers. Cadder Housing Association is included within the register of data controllers.

9.2 The GDPR requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence.

9.3 The FCSM will review the Data Protection Register with Senior Staff members annually, prior to notification to the Information Commissioner.

9.4 Any changes to the register must be notified to the Information Commissioner, within 28 days. To this end, any changes made between reviews will be brought to the attention of the FCSM immediately.

10.0 Complaints

10.1 Where any customer or stakeholder feels that the Association has either: misused their personal information; refused to allow access to information; or refused to amend alleged inaccuracies they can complain to the Association. All complaints will be handled in line with the Association's Complaints Policy and Procedure.

11.0 Breaches of the Data Protection Policy

11.1 A breach of the Data Protection Act could be a criminal offence and the Association or any individual could be liable for significant penalties.

11.2 Any breach or potential breach of Data Protection will be reported to the ICO, as set out in the Association's Privacy Policy.

11.3 The Association will develop a procedure to outline how we will manage a breach of data protection, which will outline steps including containment and recovery; assessment of risk; notification of breaches; and evaluation and response. The Association may have to investigate the actions of any stakeholder in a breach of data protection, which would be managed as outlined in section 11.3-11.9 of this policy.

11.4 Any allegations against a member of staff will be investigated thoroughly by the Finance & Corporate Services Manager (FCSM) in their capacity as the Designated Officer. If the allegation is made against the FCSM it will be investigated by the Director. If the allegation is made against a Committee member the Director will report the matter to the Management Committee for them to decide how it will be investigated. Likewise if the allegation relates to or involves the Director the Chairperson would present details to the Management Committee. The Management Committee will normally establish a Panel of members to oversee the investigation, thereafter they will report the findings to the Committee. The Management Committee may request that the Director, Auditor, Solicitor or another appointed consultant undertake the investigation.

11.5 Before any investigation begins, the Association will seek advice from Employers in Voluntary Housing or its Employment Lawyers, in relation to the alleged breach of data protection.

11.6 The member(s) of staff/Committee member(s) should be advised of the allegations and informed of what action the Association is planning to take by way of investigation. The staff/ Committee member(s) should be advised of their right to be accompanied as outlined in the Terms and Conditions of Employment or Code of Conduct, respectively.

11.7 A breach of the Data Protection Policy may be regarded as misconduct and may lead to disciplinary action through the Terms and Conditions of Employment for employees and the Code of Conduct for Committee members. In these situations it may lead to dismissal from the Association.

11.8 The Association's will follow the disciplinary procedures as outlined in the Terms and Conditions of Employment or Breach of the Code of Conduct for staff and Committee members, respectively.

11.9 In breaches of this policy by consultants, contractors, agents or partners, the Association will consider the level of breach and any recurrence to inform its decision on whether to terminate the contract.

11.10 In situations where a Committee or Senior Staff member is alleged to have breached this policy, this would constitute a notifiable event as outlined by the Scottish Housing Regulator. The notifiable event would be reported to the Regulator by the Director or Chairperson of the Association, depending on persons alleged to have breached the policy.

12.0 Training

12.1 Data protection training and awareness is essential to ensure our Committee members and staff are fully aware of their responsibilities in the management and processing of personal information, which will ensure compliance with the Policy**.**

13.0 Risk Management and Audit

13.1 There are potential financial penalties and compensation payments through failure to adhere to the relevant parts of the Data Protection legislation. Risk arises from the Association's Data Protection Policy and Privacy Policy in a number of respects:

- Failure to comply with the provisions of the data protection legislation
- Complaints from individuals about how the Association uses their personal information
- Investigation and possible action taken by the Information Commissioner
- Damage to the Association's reputation resulting from the above three factors

13.2 The Association aims to mitigate the above risk through the provision of training to staff on data protection issues. The Association will review this policy and the associated procedures on a regular basis to ensure that they meet all legislative and regulatory requirements and best practice guidance. In addition, an annual review of personal information held by the Association will be carried out to ensure ongoing compliance with the provisions of the data protection legislation.

13.3 Internal audit procedures will form an important part of establishing and sustaining good data protection practices. The Association will review the data it processes and collects and assess this against the principle as outlined in the GDPR and section 5.2 of this policy. This will inform the review of our action plan to ensure compliance with the policy.

13.4 We will undertake self assessment to periodically check our compliance with the GDPR; our Privacy Policy, Data Protection Policy, regulatory and good practice guidance; our registration with the Information Commissioner's Office; our working practices in the collection, processing and storage of personal information and achievement of our Action Plan. The results of the self assessment will

be made available to the Audit and Performance sub-committee, who will be responsible for monitoring the achievement of any recommendation.

13.5 Data protection issues will continue to be considered as part of the Association's Risk Management Strategy, and if assessed as a priority risk area in the Governance risk map or Corporate Risk Register, the commitment of resources will be considered to attend to the controls to mitigate these risks.

14.0 Policy Review

14.1 As a strategic document, the Association's Data Protection Policy will be reviewed every three years. The next review will therefore take place in May 2021 or earlier to take account of:

- Legislative, regulatory and good practice requirements;
- Association performance; or
- the views of any stakeholder in the use of personal information.

15.0 Appendices:

Appendix 1 Staff Guidance

Appendix 2 Guidance on Information a Landlord can release

Appendix 1 Staff Guidance

1.0 Staff Guidance

The GDPR establishes the principles for handling an individual's personal data.

Article 5 of the GDPR requires that personal data shall be:

- processed lawfully, fairly and in a transparent manner in relation to individuals;

- collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

- adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

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

- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

- processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number,

location data or online identifier, reflecting changes in technology and the way organisations collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

These guidelines are intended to help you handle data correctly. If you have any queries or concerns please speak to your line manager.

2.0 Keeping personal information secure

- Keep passwords secure - Change them regularly, do not share them;
- Lock/log off your computer when away from your desk;
- Dispose of confidential paper waste securely
- Take care when opening emails and attachments to prevent virus attacks
- Keep your desk clear, storing hard copy personal information securely when it is not being used
- Sign visitors in and out of the premises
- Position your computer screen away from windows, or visitors
- Avoid removing personal information out of the office unless necessary and ensure that you protect personal information which is being taken out of the office e.g. ensuring that electronic data is password protected or encrypted on a laptop, or USB memory stick

3.0 Meeting the reasonable expectations of tenants, other customers and employees

- Collect only the personal information you need for a particular business purpose
- Obtain consent to hold personal information where it is not covered by one of the other lawful basis for holding information.
- Update records promptly e.g. change of name, address
- Delete personal information that is no longer required
- Do not release personal information without consent where appropriate legitimate basis of sharing the information is not present
- Advise the Finance & Corporate Services Manager of any potential data breaches
- Where an employee or their family/friends hold a tenancy with the Association, employees will not be permitted to work on any aspect of the tenancy

4.0 Disclosing personal information over the telephone

- Do not disclose personal data over the telephone without authenticating the identity of the caller.
- In the case of a company or organisation:
  - (e.g. utility) ask for their main switchboard number and ring them back;
  - Ensure that you have a legitimate basis before releasing information to third parties.
- If it is an individual claiming to be a tenant you should run through some standard security queries using data available on the SDM Housing System regarding the tenant.
  - E.g. full name and address including postcode.
  - Names of other joint tenants (if applicable).
  - Recent rent payments (if applicable).
  - Recent repairs (if applicable)
  - Date of birth (if data held).
  - Password (if data held).

5.0 E-mail

- E-mail is not necessarily a secure way of sending information and should not be used for a sensitive, private or confidential matter.
- Staff that wish to send personal or sensitive data will need to protect the file by using a password to protect the information and by marking the email subject matter with “Private & Confidential”. Staff training can be provided on request.
- E-mails referring to an individual or organisation can be requested as part of a data subject request (either under the GDPR or the FOIA 2002 for dealings with public bodies) and staff should ensure that content is at all times accurate and reflective of Association’s Policy and that the tone is appropriate and professional.
  (Staff should note that housing associations are not regarded as “public authorities” as outlined in the FOIA 2002 and therefore not obliged to respond to freedom of information requests. The Association will nevertheless act in the spirit in the FOIA and provide information on request)

6.0 Sharing information

- You must obtain the individual’s written consent before you share information with a third party, unless it is:
  - To notify a utility services provider of the current occupant of a property;
  - To assist with the prevention or detection of crime including tackling anti-social behaviour, or;

- Requested by a Government body.
- To a third party with a legitimate reason or detailed within the Fair Processing Notice where sharing the information is required under the provision of services etc.

7 .0 What Information Should I Record and Hold?

The GDPR requires that the information you hold should be adequate, relevant, and necessary.

Relevant
We will only record or keep information that is relevant to the services being provided to individual's. If it does not relate specifically or is not relevant don't record it or keep it.

Necessary
Many of the lawful bases for processing depend on the processing being "necessary". This does not mean that processing always has to be essential. However, it must be a targeted and proportionate way of achieving the purpose. The lawful basis will not apply if you can reasonably achieve the purpose by some other less intrusive means.

It is not enough to argue that processing is necessary because you have chosen to operate your business in a particular way. The question is whether the processing is a necessary for the stated purpose, not whether it is a necessary part of your chosen method of pursuing that purpose.

Holding Information on Staff

- Only information relating to the Performance Management System and ongoing staff issues should be held by managers. All other Information should only be held on their personnel file.

8.0 Requests from Individuals to See Their Files or Personal Information

An individual has a legal right to request access to any information we hold about them. This request can be in writing or verbal.

The Association must respond to requests promptly and within 1 month from the receipt of the request.

Individuals have the right to obtain the following:

- confirmation that you are processing their personal data;

- a copy of their personal data; and
- other supplementary information – this largely corresponds to the information that is provide in a privacy notice (see ‘Supplementary information’ below).

In most cases you cannot charge a fee to comply with a subject access request.

However, where the request is manifestly unfounded or excessive you may charge a “reasonable fee” for the administrative costs of complying with the request.

You can also charge a reasonable fee if an individual requests further copies of their data following a request. You must base the fee on the administrative costs of providing further copies.

Remember that we hold personal information in a number of different formats including paper files and on IT systems such as rents, repairs (responsive and planned), allocations etc.

The individual has a right to rectify, block, erase or complete personal details if they are inaccurate or contain expressions of opinion based on inaccurate data.

You do not have to disclose data if it involves sharing data about another individual, unless that person has given their consent or there is a legitimate interest to proceed to disclose their data without their consent.

If the data relating to that other person could be redacted then that would be fine providing the other text does not give information which could result in the identification of that person e.g. in a complaint (unless the complainant has given you consent) you must not disclose their details.

9.0 Who Is Responsible For Responding To Requests For Information?

The Finance & Corporate Service Manager will have overall responsibility for responding to data subject request. As the personal data held can be spread across several systems responsibility for providing the information from the relevant areas will be as set out below:

Individual Requesting Information	**Responsible Officer**
Housing Applicant	Customer Services Manager
Tenant	Customer Services Manager

Owner-Occupiers	Customer Services Manager
Contractors	Maintenance Manager
Consultants, Agents, Partners	Relevant Senior Staff Team Member
Employees / Job Applicants	Finance & Corporate Services Manager

10.0 How Long Should Personal Data Be Kept For?

The GDPR states that personal data should not be kept for longer than is necessary for the purposes for which it is held.

The Association's Document retention Policy outline the retention periods for data held by the Association.

11.0 What Happens If I Breach Data Protection Guidelines?

Breaches of the GDPR and the Association's polices for managing personal data may result in disciplinary action.

You also may personally be liable for a fine of up to £5000 and could face prosecution if you are personally responsible for the breach.

It is essential that you report any breach or potential breach of the GDPR, the Association's polices managing personal data or the loss of personal data to your Sectional Manager and the Finance & Corporate Services Manager immediately. This will allow the Association to assess and mitigate the risks and implications of the breach. We may also require to notify the Information Commissioner's Office.

12.0 Support & Guidance

If any staff member is unsure about the disclosure of information or any other matter they should seek support and guidance from their Sectional Manager in the first instance.

Appendix 2 Guidance on Information a Landlord can release

Information Commissioner's Office
Data Protection
Good Practice Note
Disclosing information about tenants

1.0 Data Protection Good Practice Note - Disclosing information about tenants

This good practice note answers some frequently asked questions from landlords about how the Data Protection Act 1998 applies to them, the information they hold about their tenants and information held on their behalf by a letting agent.

2 .0 A landlord's legal obligations to disclose information

The Data Protection Act 1998 will not prevent a landlord from releasing personal information where they have a legal obligation to do so. For example, under the Landlord and Tenant Acts landlords may have to provide an unedited copy of the service charge account to a tenant if he or she asks for it. If so, the landlord will have to comply with the request even if it means revealing information about other tenants.

3.0 Can a landlord pass the names of new tenants to the utility companies?

Yes. A landlord has a legitimate interest in making sure that utility charges are directed to those responsible. However, landlords should tell individuals when they first agree to the tenancy that their details will be passed on.

4.0 Can landlords see references which were provided to the letting agents?

The agent can pass this information to the landlord, as long as, when the reference is asked for, they make clear to the tenant and the referee that this will happen.

5.0 Can landlords put up a list of tenants who are in arrears?

No. Information about an individual's debts should only be given out in limited circumstances. It is only justifiable to tell tenants if someone has not paid their rent if this has a direct effect on them, for example, if they become legally responsible to help meet any shortfall in shared maintenance charges.

6.0 Can landlords disclose details of a tenant who left without paying the rent?

Where a tenant leaves without paying the rent, and without making any arrangement to pay, landlords may provide their details to a tracing agent or debt collection company to help them recover money owed to them. However, it would be good practice to make tenants aware when they sign the tenancy agreement that in such circumstances this will happen. This may also help tenants think twice about not paying rent.

7.0 Can a landlord pass forwarding addresses of former tenants to the utility companies?

Yes. Sometimes a landlord will become aware that a tenant has moved leaving behind an unpaid utility bill or an account in credit. In addition a utility provider may need to contact a former tenant regarding continuing social support. In these circumstances landlords can pass a forwarding address (where known) to the utility companies as the Act is not intended to be an obstacle to disclosure in these situations. However, landlords must make tenants aware of these possible disclosures at the start of the tenancy.

8.0 Giving out information

In general, landlords should make clear to tenants when they sign the tenancy when and how their information will be given out. However, if an emergency repair needs to be carried out, it would not breach the Act to go ahead and provide tenants' contact details to the repairers. On the other hand, if a domestic contractor is looking for work the tenants should be left to contact the contractor rather than the landlord giving out the tenants' details without their knowledge or agreement.

9.0 Good practice checklist

Before you give out information, consider the following points to help make sure you are giving out the information fairly.

- Whether the information you want to give out is personal information
- Whether you have told the tenants that you may give out this information, and in what circumstances
- Who you are giving the information to and why they want it
- Any legal obligation to give out the information
- Whether it is really necessary to give out the information

10.0 More information

If you need any more information about this or any other aspect of data protection, please contact us:

Phone: 01625 545745
E-mail: mail@ico.gsi.gov.uk
Website ww.ico.gov.uk