

Confidentiality GDPR Policy

INTRODUCTION

This policy sets out Robert Denholm House's approach to the General Data Protection Regulation 2018 (GDPR) and applies to all personal data held by the Robert Denholm House relating to any identifiable living person.

Personal information held about our customers will be handled sensitively and confidentially by all staff, agents and Members of our Committees and Boards. It should be noted that customers may be past, present and future tenants, leaseholders or others with whom we have dealings, including data held on past, present and future staff.

POLICY STATEMENT

All employees, Board and Committee Members and agents must comply with this policy.

In doing so, they will:

- Treat all personal and sensitive information as confidential.
- Comply with the law regarding the protection and disclosure of information.
- Not disclose information without the prior informed consent of the individual concerned, except in the circumstances detailed below under "disclosure" or where otherwise permitted by the law.
- Not attempt to gain access to information they are not authorised to have.

All personal information about customers of Robert Denholm House and its subsidiaries will be:

- Obtained, held and processed fairly.
- Held for specific purposes and used only for those purposes (these should be the same as stated in our Data Protection Notification).
- Relevant, accurate and kept up to date.
- Corrected if shown to be inaccurate.
- Kept no longer than is necessary and destroyed when no longer required, in line with best practice.
- On request, made available to the data subject.

OBJECTIVES

- To ensure compliance with the GDPR and regulatory requirements in relating to confidentiality.
- To ensure all staff across the Robert Denholm House are aware of, and understand the importance of, data protection and confidentiality.
- To ensure the protection of personal and sensitive information of staff and customers.
- To ensure customers are able to have access to their own information within relevant timescales.

- To annually review the disclosure categories as part of the Data Protection Registration process.
- To ensure procedures are in place across the Robert Denholm House partners for staff, contractors and Board and Committee Members regarding disclosure of personal information.
- To ensure all staff receive appropriate data protection training, with regular updates or when significant data protection guidance changes.

RESPONSIBILITIES AND REQUIREMENTS

1. All staff have a responsibility to effectively manage personal data. Managers should ensure all their staff receive adequate training as described above.

2. Personal information must be treated as confidential and must only be disclosed for purposes that are notified to the Information Commissioner's Office (formerly known as the Data Protection Registrar), to:

- Employees of the parent or partner associations, where the information is necessary for their work
- Others in accordance with the Data Protection notification.

3. All computerised and manual filing systems containing data relating to any identifiable living person must be documented in the Data Information Asset Register which ensures the data is:

- identified, including where it came from, is stored, who it has been shared with, whether consent has been given
- secured
- accurate and kept up to date and retained only so long as required
- notified to GUHG's designated Data Protection Officer (Head of Governance and Business Services).

Such systems must be designed and operated so as to comply with the Data Protection principles.

4. Any person may ask Robert Denholm House for the data that the parent or partner associations hold about them. Any such request should be immediately passed to the Data Protection Officer for action (a response must be made within 30 calendar days). Any data that the person is entitled to see must be presented in plain language in hard copy format. Additionally, where necessary, the information will be provided verbally.

From 25 May 2018 subject access requests (SAR) are provided free of charge.

5. Any breach in the policy must be reported immediately to the Data Protection Officer. A breach could have very grave consequences for an individual or the Group and will be treated as a serious matter. Disciplinary action, including dismissal in a serious case, will be taken against any employee of Robert Denholm House who commits a breach of this policy. The employee may also be open to criminal proceedings that may result in an unlimited fine or a custodial sentence.

ACCESS TO INFORMATION AND DISCLOSURE OUTSIDE THE GROUP

Staff across the Robert Denholm House team will generally have access to all the information they need to carry out their work and they have a duty to keep that information confidential. In the unlikely event that any information needs to be disclosed to someone outside the Robert Denholm House, staff must explain to an individual why this is necessary and obtain written consent before doing so. If an individual does not give consent, this should be noted and special arrangements should be made for recording information and access to it. However, relevant agreements and protocols are in place that allow for the exchange of information between the Robert Denholm House and the relevant Local Authorities in relation to the processing of housing applications and in the prevention of crime and anti-social behaviour. There are certain situations where, by law, staff do not have to obtain prior permission to disclose personal information about individuals.

These are:

- To comply with the law (e.g. the police, Inland Revenue, Council Tax Registration Office or a court order).
- Where there is a health and safety risk (this will include information about customers with a history of violence and when other care professionals are involved in a customer's care).
- When there is evidence of fraud.
- In connection with court proceedings or statutory action to enforce compliance with tenancy conditions (e.g. applications for possession or for payment of Housing Benefit directly).
- The name of a customer and the date of occupancy to utility companies (where the customer is responsible for direct payment), providing the customer has agreed to this at the start of the tenancy or has given consent to the passing on of the information since.
- Anonymously for bona fide statistical reporting or research purposes, providing it is not possible to identify the individual to whom the information relates (e.g. CORE returns).
- Where specifically enabled by the terms of registration of the GDPR.
- Where there are declarations of interest by staff, Committee or Board members.
- Where any staff may have concerns about a customer under the Safeguarding of Adults from Abuse policy, or related concerns under the Safeguarding Children policy.

Any information disclosed must be necessary for the purpose for which it is disclosed. Therefore, staff should not, for example, disclose details of a tenant's religious beliefs if only their name and contact details are needed for the purpose of carrying out repair work. If it is necessary to discuss individual customers at meetings involving people from outside the association or to refer to them in reports, it is suggested that they could be referred to by codes, e.g. Tenant A, to maintain anonymity.

DISPOSAL

All personal information will be destroyed as soon as practicable when it is no longer needed. The method of disposal should be appropriate to the confidentiality of the information in accordance with the Group Data Protection Guidance.