UK General Data Protection Regulation (UKGDPR) Policy

Document Control

Responsible Person	Chief Executive			
Review Frequency	5 Yearly			
Reviewed by	Board			
Date Approved	November 2023			
Next Review Due	November 2028			
Consultation Required	Yes		No	✓
Equalities Impact Assessment	Yes	✓	No	
Added to Company Website	Yes	✓	No	
Associated Documents Considered	Yes	✓	No	

1. Introduction

1.1. The company holds large amounts of personal data which is used by many people in the course of their work. The company has a duty to ensure the confidentiality of such data in all formats and aims to comply with the legal requirement of the UKGDPR and any subsequent or relevant legislation.

2. Background

2.1. The company recognises the UKGDPR is an important piece of legislation to protect the rights of individuals in respect to any personal information that we may keep about them, whether electronically or in manual systems.

2.2. We are registered with the Information Commissioner as a Data Controller under the UKGDPR and must ensure that our practices in the handling of personal information are of a high standard and are fully compliant.

3. Principles

3.1. The company will adopt and operate procedures in compliance with UKGDPR, as listed below. Personal information and data held by the Company shall be:

a) obtained and processed fairly, lawfully and in a transparent manner.

b) collected only for the specified, explicit and legitimate purposes, and shall not be further processed in a manner that is incompatible with those purposes.

c) adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

d) accurate and where necessary is kept up-to-date, with every reasonable step taken to ensure that inaccurate data, having regard to the purposes for which it is processed, is 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 it is processed.

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.

3.2. The Board and all staff who process any personal and sensitive information must ensure that they follow these principles at all times. Training will be provided on the principles and the company's procedures for data protection to all relevant personnel on a regular basis. New staff will have this incorporated into their induction process.

4. Responsibilities

4.1. The Chief Executive has overall responsibility for the data protection within Waverley Housing, and for ensuring that our notification to the Information Commissioner, and our entry in the Data Protection Register is accurate and up to date.

4.2. The Data Controller is the organisation that is responsible for:

a) Ensuring and being able to demonstrate that its processing is performed in accordance with the UKGDPR

b) Ensuring Implementation of this Data Protection Policy and associated procedures

c) Maintaining a register of all processing activities, taking account of the appropriate legal grounds for lawful processing of data

d) Fulfilling any personal data breach notification duties

e) Completion of a Data Protection Impact Assessment for any new data processing activities deemed to result in high risk

f) Selecting and working only with data processors who have the right safeguards in place

g) Taking into account special data categories and the special rules regarding the personal data of children, including the need for explicit consent

h) Delivering on duty of information, also when the personal data have not been obtained from the data subject

i) Facilitating the exercise of data subject rights

j) Liabilities for damage caused by processing which infringes the UKGDPR and leads to penalty

k) Appointing a Data Protection Officer.

The Data Protection Officer is responsible for:

a) Informing or advising the Data Controller and the employees who carry out processing of their obligations of UKGDPR.

b) Monitoring compliance with UKGDPR in relation to the protection of personal data, including responsibilities, awareness-raising and training of staff involved in processing activities, and related audits.

c) Providing advice where requested as regards data protection impact assessments and for consulting with the Information Commissioners Office (ICO) where high risk is identified prior to proceeding with the activity.

d) Co-operating with the ICO and to act as the contact point with them.

4.3. The Executive Assistant (HR) has specific responsibility for personal and sensitive information held on employees and the Executive Assistant (Governance) in respect of board members. Staff and board members are informed about data protection principles.

Our Privacy Policy and Fair Processing Notices for tenants and other customers, and for employees/board members sets out our processing, sharing and security of personal data held, and rights to access personal data.

4.4. Operational Managers will ensure personal data processed by their sections is included in the company's Data Processing Activities Register, and for ensuring this is kept up to date and compliant with the above principles.

4.5. All employees and board members have a responsibility to protect the personal information held by Waverley Housing. They will take steps to ensure that this is kept secure at all times against unauthorised or unlawful loss or disclosure and in

particular will ensure that:

a) They are appropriately trained in the handling of personal and sensitive information.

b) Paper files and other records or documents containing personal/sensitive data are kept in a secure environment.

c) Personal data held electronically is protected by the use of secure passwords which, where possible, have forced changes periodically; that screens cannot be seen by tenants/visitors and that screens are not left 'logged in' when unattended.

d) All mobiles have a passcode to access the handset and that Corporate Services are notified in the event of the handset being lost or stolen, to enable data on the handset to be wiped.

e) They check the identity of people before discussing information by phone or disclosing information in a face-to-face interview or home visit.

f) They only disclose personal data internally to those people with a 'right to know'.

g) They dispose of documents containing personal or sensitive data as Confidential Waste where its purpose has been served or in accordance with our Data Retention Periods.

h) If and when, as part of their responsibilities, employees or board members collect information about other people, they must comply with the guidance set out in this policy. No one should disclose personal information outside this guidance or use personal data held on others for their own purposes.

i) It is a standard condition of Waverley Housing contracts that our agents and sub-contractors will comply with the law on UKGDPR.

5. Access Rights

5.1. Tenants, employees and other individuals about whom the Company holds personal information will have the right to access their information, unless it is exempt under the UKGDPR.

6. Confidentiality

6.1. All staff have restricted and passworded access to ensure information is only accessible to those who need to know the information in order to carry out the requirements of their post.

7. Failure to Observe this Policy

7.1. Any person who breaches this policy may find themselves facing, in addition to disciplinary action, criminal charges.

8. Breach Reporting

8.1. In complying with the UKGDPR Waverley Housing requires to keep a record of all data breaches and the resultant investigations.

8.2. Any member of Waverley Housing staff who considers that a breach may have occurred, where personal or sensitive data has been lost or released to a third party

without authority, must inform the Data Protection Officer (DPO) immediately.

8.3. The DPO will record the details of the incident in the Data Breach Register and start an investigation into it. The details of this investigation will also be recorded together with any outcomes.

8.4. Should the breach be found to have occurred, the DPO will notify the relevant parties, in accordance with the requirements of UKGDPR. Where a serious breach has occurred the Chief Executive should be notified immediately and the breach treated as a notifiable event and reported to the Scottish Housing Regulator.

8.5. Remedial action will be taken by the DPO, to ensure that the data is restored and/or recovered and that all relevant parties are consulted with and notified.

9. Training

9.1. Waverley Housing will ensure that all employees and board members have the appropriate level of skills and knowledge to deliver the requirements of this policy.

10. Reporting

10.1. The DPO will report to Management Team on any Data Protection issues including breaches arising. The Board will be notified of any serious breach.

11. Data Auditing and Review

11.1. The DPO will monitor compliance with this procedure through selective audits of records

11.2. A copy of the Data Processing Activities Register will be issued to Operational Managers annually who should ensure that the information recorded is accurate and up-to-date. This Policy will be subject to review in accordance with our Policy Review Listing.