GENERAL DATA PROTECTION REGULATION (GDPR)

Principles, Roles and Responsibilities

The Principles

Waverley Housing will adopt and operate procedures to ensure compliance with the principles of GDPR listed below. Personal information and data held by us shall be:-

- Obtained and processed fairly, lawfully and in a transparent manner
- Collected only for specified, explicit and legitimate purposes, and shall not be further processed in a manner that is incompatible with those purposes
- Adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed
- 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
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which it is processed
- 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 Board and all employees who process any personal information must ensure that they follow these principles at all times. Training will be provided on the principles and our procedures for all relevant personnel on a regular basis. New staff and board members will have this incorporated into their induction process.

Roles and Responsibilities

The **Chief Executive** has overall responsibility for 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.

The **Data Controller** is the organisation (Waverley Housing) that is responsible for:-

- Ensuring and being able to demonstrate that its processing is performed in accordance with the GDPR
- Ensuring implementation of our Privacy Policy, Fair Processing Notices and other associated procedures

- Maintaining a register of all processing activities, taking account of the appropriate legal grounds for lawful processing of data
- Fulfilling any personal data breach notification duties
- Completion of a Data Protection Impact Assessment for any new data processing activities deemed to result in high risk
- Selecting and working only with Processors who have the right safeguards in place
- Taking into account special data categories and the special rules regarding the personal data of children, including the need for explicit consent
- Delivering on duty of information, also when personal data has not been obtained from the data subject
- Liabilities for damage caused by processing which infringes the GDPR and leads to penalty
- Appointing a Data Protection Officer.

The **Data Protection Officer** is responsible for:-

- their obligations of GDPR
- Monitoring compliance with GDPR in relation to the protection of personal data, including responsibilities, awareness-raising and training of staff involved in processing activities, and related audits
- Providing advice where requested as regards Data Protection Impact Assessments and for consulting within the Information Commissioner's Office (ICO) where high risk is identified prior to proceeding with the activity
- Co-operating with the ICO and to act as the contact point with them.

The **Executive Assistant (HR)** has specific responsibility for personal information held on employees and the **Executive Assistant (Governance)** in respect of Board Members.

Staff and **Board Members** responsibilities for compliance:

All staff and board members, particularly those tasked with regularly handling personal data of colleagues or third parties, have responsibility for ensuring that processing meets the standards set out in our Privacy Policy and Fair Processing Notices. They must observe, as a minimum, the following rules:-

- Observe to the letter any instruction or guidelines issued by Waverley Housing in relation to Data Protection in accordance with the principles outlined above
- They should not disclose personal data about the company, colleagues or third parties unless that disclosure is fair and lawful and in line with our Privacy Policy and the above data protection principles
- They must take confidentiality and security seriously, whether the staff or board member considers the information to be sensitive or not

- Any personal data collected or recorded manually which is to be inputted to an electronic system should be inputted accurately and without delay
- They must not make any oral or written reference to personal data held by the Company about any individual except to staff or board members who need the information for their work or an authorised recipient
- Great care should be taken to establish the identity of any person asking for personal information and to make sure that the person is entitled to receive the information
- If a staff or board member is asked by an unauthorised individual to provide details of personal information held by the company, they should ask the individual to put their request in writing and send it to the Data Protection Officer. If the request is in writing, this should also be passed to the Data Protection Officer
- Staff or board members must not use personal information for any purpose other than their work for the company
- If a staff or board member is in doubt about any matter to do with data protection, they must refer the matter to the Data Protection Officer immediately and before progressing
- Passwords should not be disclosed and should be changed regularly
- Staff, board members or third parties' personal data should not be left unsecured or unattended, e.g. on public transport, within cars or trades vans etc
- Unauthorised use of computer equipment issued by the company is not permitted
- Staff members must follow the company's Clear Desk practice and ensure that all confidential information, whether containing staff member or third party personal data or not, is secured when it is not in use or when the staff member is not at work
- Staff or board members may only use equipment to carry out work, where work is encrypted and/or password protected, ensuring all devices are password protected and locked when not in use;
- Emails containing staff or board member or third party personal data must not be sent from a web-based email system
- As far as is possible, staff or board member or third party personal data contained in emails and attachments should be anonymised before it is sent by email
- All documents containing sensitive information should be password protected and, if the document requires to be transmitted, the document and password should be transmitted separately.

Any breach by staff or board members of the above rules will be taken seriously and, depending on the severity of the matter, may constitute gross misconduct which could lead to summary termination of employment or board membership.