The Wrekin Housing Group	**Data Protection and Confidentiality Policy** **Policy no.**

1. Policy Statement

The Wrekin Housing Group ("the Group") is committed to conducting its affairs openly, and will take all reasonable steps to ensure that its tenants and service users have access to appropriate information regarding the Group and its activities.

The Group as a company, landlord, care provider, service provider and employer holds a large amount of personal data and is committed to protecting the privacy of all individuals by ensuring compliance with the relevant data protection legislation. The Information Commissioner, an independent body, is responsible for enforcing data protection law. The Group is registered as a data controller with the Information Commissioner. Responsibility for completing the annual registration lies with the Head of ICT who is also the Group's registered Data Protection Officer.

Rights to privacy and confidentiality enjoyed by tenants, applicants, service users, employees, officers and contractors will be protected to ensure that personal information relating to them is dealt with confidentially and sensitively, and in accordance with the relevant legislation. Likewise, the confidentiality of commercially sensitive information relating to its own and other businesses will be preserved.

All Group business will be conducted in accordance with the terms of the General Data Protection Regulations 2016, and all personal data will be handled in accordance with the 'Six Principles of Data Protection' as contained in the Regulations.

Data protection principles cut across all Group activities and guidance is available in the Group's Data Protection and Confidentiality Procedure. More specific guidance relating to particular areas of Group business is provided in additional policies and procedures. These include:

- Employment - covered in the Recruitment and Selection Policy and Procedure and also in the Guidance Notes on Obtaining References.
- Data security and handling – covered in a suite of policies and procedures managed by the ICT Consultancy. These are detailed in the implementation section of this policy.
- Information sharing – the Group enters into a number of information sharing protocols for example, with the Police and different Local Authority departments.

Definitions of key terms relevant to this policy are contained in the implementation section.

2. Roles and Responsibilities

The Group Head of Legal and the Group Head of ICT are responsible for implementing relevant procedures.

The Legal Team delivers part of the induction programme for new starters and are responsible for the delivery of information relating to Data Protection and Confidentiality.

Managers are responsible for providing basic information and training to all employees regarding confidentiality and data protection.

All employees have individual responsibility for implementing this policy and adhering to all associated procedures.

3. Confidentiality and Data Protection Policy Implementation

Definitions

The following definitions apply with reference to this policy:

- Personal Data – data concerning an individual who can be identified from the data or any other accessible information, including (but not limited to): name, address, date of birth, image;
- Sensitive Personal Data – personal data including (but not limited to): medical information, sexuality, ethnicity, trade union membership, religion, immigration status, criminal record, information collected as part of an investigation into anti-social behaviour or abuse;
- Data Subject – the living individual whose personal information is collected and processed;
- Data Controller – the legal entity (organisation or individual) with responsibility for the collection and management of personal information. Data Controllers will usually be organisations, but can be individuals, for example, self-employed consultants. If an individual is given responsibility for data protection in an organisation, they will be acting on behalf of the organisation, which is the Data Controller;
- Data Processor – the organisation or person who processes personal information on behalf of the Controller;
- Processing – how personal information is collected, used, recorded, stored, shared, disclosed, altered, erased, made available or destroyed;
- Breach – a breach of security leading to accidental or unlawful loss, destruction, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
- Commercially Sensitive Data – Any information not publicly known, which relates to the business of the Group or any contractor or tenderer.

Information to be kept confidential

The following categories of information are to be kept confidential:

Personal data and sensitive personal data - not to be disclosed outside the Group except as in paragraph 3 and disclosed inside the Group only when necessary.

Commercially sensitive data – the Board and Executive Management Group will ensure that all employees are aware of the aims, activities and plans that may affect them.

Board papers and minutes - will be confidential and not made available unless the Board, or the persons designated by the Board, decide otherwise.

All financial information relating to the Group's performance is commercially sensitive data and not to be disclosed outside the Group except to regulatory bodies that require the data to fulfil their function, and except to the extent published with the Board's authority.

Disclosure

Disclosure of personal data, sensitive personal data or commercially sensitive data relating to another person is permitted where:

(i) The Group has the consent of the individual or a request from the individual.
(ii) Legislation permits or requires disclosure.
(iii) The recipient is an advisor or auditor with a professional duty of confidentiality.
(iv) The recipient is a statutory body carrying out a public service or function.

Disclosure of commercially sensitive data relating to the Group is permitted where directed by the Board or the persons delegated by the Board for the purpose of this policy.

Data Processing and Security

The Group will implement relevant procedures to ensure the security of personal data, sensitive personal data and commercially sensitive data in whatever form it is held.

All Group staff will be bound by the Group's policy on confidentiality and data protection, and adherence to this policy will be a condition of employment contained within the contract of employment. Breach of this requirement is a disciplinary offence. Contracts for goods and services will also normally contain a clause requiring that confidentiality be maintained, and where the sharing of personal information is necessary for the performance of the contract, a Confidentiality Agreement must be entered into.

All personal data and sensitive personal data held by the Group will be relevant, accurate and related to the purpose for which it is held and will not be kept any longer than is necessary for the purpose for which it was collected.

Managers who are delegated as data controllers will be notified of any changes in the way personal data, sensitive personal data or commercially sensitive data is processed.

Disposal of Data

The Group will implement a relevant procedure for the disposal of personal data, sensitive personal data and commercially sensitive data when no longer required. Guidance on document retention is contained in the Group's Data Protection & Confidentiality Procedure.

Accessibility

The Group will:

- Respond to a reasonable request for information and make available data that is not personal data or sensitive personal data or commercially sensitive data within a reasonable time;
- Ensure information is provided in a comprehensive and non- discriminatory way that meets the special needs of tenants, service users and other key stakeholders;
- Comply with legal and regulatory requirements to provide information.

4. Related Policies and Procedures

Guidance on the implementation of data protection is not restricted to the Group's Data Protection and Confidentiality Policy and Procedure. Many other policy and procedure documents contain specific guidance in relation to particular aspects of data handling and these should always be considered together. These include, but are not limited to:

ICT and Data Protection Policies

- Portable PCs, PDA and Digital Camera Policy;
- IT Security Policy;
- Information Security Management System Policy;
- Cyber Security Incident Response Plan;
- Subject Access Request Policy & procedure.

Human Resources Policies

- Recruitment and Selection Policy and Procedure;
- Guidance Notes – References.

Tenancy Management Policies

- ASB Policy;
- ASB Procedure;
- Information Sharing Agreement (Police);
- CCTV Procedure Statement;
- Allocations & Lettings Policy;
- Data Loss & Information Security Breach Reporting Policy & Procedure;
- Subject Access Request Policy & Procedure;
- Consent to Care and Treatment Policy;
- Mental Capacity Policy (Choices).

Policy Category	Data Protection
Approved by **Date**	Executive Management Group 10th May 2018
Implementation date	May 2018
Review date	February 2021
Expiry date	May 2021