Data Protection and Confidentiality Policy

Issue No:	2
Responsible Officer:	Maryjane Elder (SCSO)
Author:	Maryjane Elder
Date Last Amended:	January 2012
Date Effective From:	March 2018
Review Date:	March 2023

Data Protection and Confidentiality Policy

Introduction
This policy sets out the Ore Valley Group (OVG) approach to the General Data Protection Regulation 2018 (GDPR) and applies to all personal data held by the Group relating to any identifiable living person. It provides a framework under which the Ore Valley Group should conduct its normal activities, so that the GDPR (2018) is complied with fully.

This policy covers data protection and confidentiality for customers, tenants & staff. All staff are expected to act with due care and diligence with regards to the protection of personal information, but may from time to time have to make value judgments in certain situations. Any such judgments should be made with reference to this document and further, specifically the eight data protection principles noted below. If in doubt, staff must contact their line manager who will escalate as necessary.

Personal information held about our customers will be handled sensitively and confidentially by all staff, contractors, agents and Members of our Board and Committee.

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.

In addition, the document is designed to ensure that only those member of staff who are required to input and make amendments to data will be able to do so.

Policy statement
All employees, Board and Committee Members, contractors and agents **must** comply with this policy, the Group's Data Protection Guidance and Clear Desk Procedure in addition to the GDPR. 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.

Types of data subjects
Ore Valley Group may hold information on current/ex/prospective customers, tenants and staff as well as other individuals such as suppliers, advisers and visitors. Individuals who are a subject of data are known as

"data subjects".

Types of data
The Ore valley Group may hold two types of what the GDPR terms "personal data":

Personal data: this covers both facts and opinions about an individual and therefore includes case notes as well as other information that may help us identify individuals. It also includes indication of intentions in respect of individuals. Examples include name, address, age, date of birth, financial details, supplier details, health and safety and security details.

Sensitive personal data: including race or ethnicity, religious or similar beliefs, physical or mental health, political opinions, trade union membership, sexual life including sexual orientation, offences/alleged offences and information about criminal proceedings including sentencing. This data is specially protected under the Act and cannot normally be processed without the data subject's consent.

Personal data and sensitive personal data may be held in electronic or paper form. We also hold information which is not personal or sensitive personal data. We call that "anonymous information" (please refer to ICO guidance):

Anonymous Information is all non-private information, including amongst other things; the anonymous content of any day-to-day work, including statistics produced as part of performance management. Such information must not include references to individual customers or information that may allow a customer to be identified, unless that customer's permission has been obtained (in which case the information will not be anonymous but will be personal or sensitive personal data). If you are unsure whether information is anonymous or personal, please contact your line manager who will escalate as necessary.

Data Protection Principles
All personal information about customers of the Group and its subsidiaries will be:

- Processed fairly and lawfully and with a legal ground for processing
- Held for specific purposes and used only for those purposes (these should be the same as stated in our Privacy Statement)
- Adequate, relevant and not excessive
- Accurate and up to date
- Kept no longer than is necessary and destroyed when no longer required, in line with best practice
- Not be transferred to other countries outside the EEA without adequate protection against loss or disclosure and in accordance with the Clear Desk procedure and Data Protection Guidance
- Kept securely
- 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 Group 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 Group 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.

Other Related Policies

Clear Desk Procedure
Data Protection and Confidentiality policy
Equality and Diversity Policy
Privacy Notice
Fair processing Notice
Employee Fair Processing Notice

Responsibilities and Requirements

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

- All computerised and manual filing systems containing data relating to any identifiable living person must be documented in the Data Information 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 the Ore Valley Group designated Data Protection Officer

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

- Any person may ask The Ore Valley Group for the data that is held 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.

- 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 the Group 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 Group 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 Group, 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 Group 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 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.

Data Storage and Processing Personal information must be stored confidentially and securely in both computer databases/on computer media and manual filing cabinets.

Personal information must only be available to authorised staff and you must not disclose it either orally or in writing to any unauthorised third party. It is a condition of employment that all staff members comply with this policy. Agents, contractors and other temporary staff must also comply.

You must never store personal information on the hard drives of laptops for longer than it takes to gain a connection and import onto the network. All laptops and other portable devices and media such as USB memory sticks must be encrypted.

It is accepted that in order to obtain customer's signatures, original and complete documentation may need to be taken out of the office, also. It is imperative that all staff carrying paperwork with them does so in a secure and responsible manner and with prior knowledge of their line manager; it is vital that any data must not be left visible.

Full case records and other information (including 3rd party) may be removed from the office in exceptional circumstances only on the authorisation of their line Manager.

Whilst records are out of the office, it is the member of staff's responsibility to ensure they are not left unattended, that they are kept secure at all times and returned to the office as soon as possible.

Referrals made to the Housing Team via email should only be sent and received via a secure method i.e. OVHA official email accounts, FORT System, FHR etc. Referring agencies must be informed that we cannot accept referrals via any other potentially non-secure electronic method.

Signs should be displayed in each area, where relevant, informing that CCTV is in use. All tenants should sign the document enclosed in the sign up pack explaining why CCTV is in use and what the Ore Valley Group may do with the data.

Sharing Information with others
Third Parties
There is no breach of confidentiality if the individual (who has capacity) agrees in writing to information being given to a third party. When a third

party approaches the Ore Valley Group with an enquiry on behalf of a customer for that customer's information, the third party must be given consent form, and return it, signed by the customer, before any information is released.

Death of a customer/Tenant/Staff Member
Death does not end the Ore Valley Group duty of confidentiality to the customer/tenant/staff member. If an individual has died, confidential information relating to that individual and held by the Ore Valley Group can only be given to someone who is a personal representative of the deceased and who has a grant of representation (i.e. a grant of probate or grant of letters of administration) or an indemnity. The Ore Valley Group must ask to see the original or office copy grant of representation/indemnity and retain a copy on file.

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.

Our Retention Policy should be followed regarding retention and disposal.

Monitoring
- The Executive Management Team of The Ore Valley Group is required to ensure compliance across the Group with this policy.
- The Senior Management Group will be accountable for the management of data protection within the Group.

Any complaints made relating to breaches or possible breaches of confidentiality will be reported to the CEO for investigation and recorded on the Data Protection Log.

This policy will be monitored as part of the annual policy review programme.