Data Protection & Information Security Policy

Introduction
The purpose of this policy is to ensure that:

- All personal data held by the Association will be processed lawfully and will only be used for the purposes for which it was collated.
- Only authorised personnel will have access to information. Staff will only have access to information they require for the purposes of carrying out the duties of their post.
- The Association has systems in place to recover data should it be accidentally lost, damaged, or destroyed.

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

Reference
Reference should be made to the Data Protection Act 1998 and the Freedom of Information (Scotland) Act 2002. Further details can also be obtained by visiting the Scottish Information Commissioner website at www.itspublicknowledge.info/legislation.htm

Data Collection and Processing
The Association will initiate procedures to ensure adherence to the following principles of legislation.

- All personal data will be processed fairly and lawfully.
- Personal data will only be used for the purpose for which it was collected.
- The personal data held on record will be adequate, relevant and not excessive in relation to the purposes for which they are processed.
- Personal data shall be accurate and, where necessary, kept up to date.
- Personal data will not be kept for longer than is necessary for the purpose for which it was collected.
- Personal data will be processed in accordance with the rights of the data subjects under the legislation.
- Right of access to personal data held on them.
- Right to stop or prevent processing likely to cause unwarranted substantial damage or distress.
- Right to compensation.
- Right to obtain rectification, blocking, erasure or destruction of inaccurate data.
- Right to request the Data Protection Commissioner to assess whether personal data is being processed lawfully.
- Appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against loss or destruction of, or damage to, personal data.

Access to Personal Information

All staff and any other person whose personal data (personal information about a living individual who can be identified from that information and other information which is in, or likely to come into, the data controller's possession) the Association processes (processing means obtaining, recording or holding the data or carrying out any operation or set of operations on data. have the right to:

- Be informed what personal data about them the Association holds and what it is used for
- Access this personal data
- Update the personal data the Association holds
- Be informed how the Association is complying with its obligations under the Data Protection Act (DPA)
- Complain to the Corporate Support Officer if they feel that the Data Protection Policy has not been followed

Access to Information

The Association has procedures in place outlining which members of staff have access to process data, to read data and those members who have no access to data.

Appended to this document is information outlining the access to data afforded to each member of staff. At no time should this access be altered without the prior approval of the Director.

Storage of Data

- Confidential information relating to prospective, current and former tenants, contractors and suppliers is held on the housing database, the main file system, the e-mail system and manual files.
- Confidential information will only be accessible to staff who 'need to know' such information in order to carry out their duties.
- Confidential information will be kept discreetly at all times, out of view of visitors to the office or other staff and contractors who do not need access to the information in order to carry out their duties.
- Files will be suitably stored and will not be removed from the office unless absolutely necessary. If files are removed from the office then they will remain in the control of that member of staff, kept secure and not visible to other persons.
- Members of staff, applicants for housing, tenants, leaseholders and any other visitors will be offered a private place to discuss matters of a confidential nature.
- Where there is a requirement to discuss confidential information internally, this will be done in private and only between members of staff who have a legitimate right to access that information in order to carry out their duties
- At the end of the working day, all confidential information will be moved out of view and wherever possible put away in desks and filing cabinets.
- When dealing with customers by telephone the Association will take steps to ensure the identity of the individual before disclosing personal information.
- Employees will not discuss confidential information with third parties who have no particular right to know about the internal business of the Association.
- The Association will give anonymity to tenants wherever practicable in reports to the Board.
- Confidential information relating to all prospective, current and former employees and the Board is held securely by the Director and Corporate Support Manager

General Security
The following procedures are to be used by all staff.

- All staff with access to computer data will be required to change their passwords on a regular basis. On no account should passwords be divulged to other members of staff. Further protection is enabled using multi-factor authentication such as via a work mobile phone.
- When leaving their workstations, staff will ensure that they either log off or lock their PC.
- Procedures are in place to ensure that staff have access to all data they require to enable them to carry out their duties of their post. At no time should staff be using a PC which has been accessed by another member of staff.

Incident Reporting
There is a formal procedure for reporting, investigating and recording Information security incidents. All incidents should be reported to the Corporate Support Manager who will investigate immediately.

Internet Access
Those members of staff who have access to the internet will only use this for the purposes of obtaining information directly relevant to the Association.

Access to the internet for any other purpose must be authorised by the Director or Corporate Support Manager. ***(Please refer to the Association's Email and Internet Usage Policy for further details)***

Email
All members of staff will have access to Email facilities. The Chief Executive and the Corporate Support Manager will undertake periodic audits of email with assistance from the Association's IT support provider. This may involve checking individual employee's email via access at the exchange server. All staff are aware that any form of e-mail or other electronic information gained through periodic checks or accessed by the Association to corroborate instances of suspected fraud, bribery, whistle blowing or other breech of terms and conditions will be used by the Association for the purposes of disciplinary action.

It is a disciplinary offence to use Email for the purposes of sending rude or offensive messages. ***(Please refer to the Association's Email and Internet Usage Policy for further details)***

Sharing of Information
The Association has developed a Communications Strategy for sharing information with other organisations such as the Local Authority, Police etc.

Data Recover
The Association has systems in place to ensure that data can be easily recovered in the event of accidental loss or damage.

- Back-ups are taken on a constant basis. Backups are undertaken utilising cloud-based systems that constantly backup the Association's data. These are maintained and overseen by our respective IT service providers.

- In the event of an incident resulting in the damage to or the loss of data, the Association's support provider would be in a position to totally restore the system within 24 hours as outlined in the Business Continuity Plan and also the Disaster Recovery Plan .

Performance, Performance, Measures and Targets

- Data Protection Audits will be undertaken a six-monthly basis and the outcomes of these audits will be monitored and appropriate action taken if weaknesses are identified.
- Complaints that are received with regard to Data Protection and any associated compensation payments will be monitored.
- Results of the monitoring exercises will be reported to the Finance, Audit And Risk Management Committee on an annual basis. In the event of serious breaches, these will reported at the next scheduled meeting.

Data Protection Registration

The Association is registered with the Data Protection Act 1998 – **Registration No: Z5454706, Security No: 10213946**. This registration is renewed on an annual basis through the Information Commissioner. Copies of the Association's Registration can be found within the main filing system on file 10.8

Monitoring and Review

The effectiveness of this policy will be reviewed on a three yearly frequency unless legislation, regulation, or monitoring exercises dictate otherwise.

APPENDIX 1

Access to Information

System Directory
All staff have access to the Association's Microsoft SharePoint/OneDrive system which is segregated depending upon staff member access requirements All staff have access to the main 'OVHA – Documents' SharePoint system which contains sub-folders named as follows:

- CHAP Cloud
- General
- OV Energy Cloud
- OV Enterprises Cloud
- OV Heating Cloud
- OVCI Cloud
- OVHA Cloud
- Sage Backups
- SDM

A second primary SharePoint is accessible to senior management only named 'Personnel – Documents'

Appendix 2 - Access to Information Within HomeMaster

OVHA utilises HomeMaster for hosting its housing management system. This system is entirely cloud based and accessed via a browser. Data is stored, retained and protected by HomeMaster on OVHA's behalf as part of the service agreement.

Staff access is controlled by and linked with their existing Microsoft user accounts and access and utilisation limitations are put in place by OVHA to control limits on data access, authorisation levels, operation processes etc. These limitations are varied depending upon role and responsibilities. These are outlined as on the separate spreadsheet.

APPENDIX 3

Awareness Guidance

Data Protection Act 1998 (DPA)
The Data Protection Act 1998 (DPA) enables individual access to information to which they are the subject e.g. someone's own education/medical records, credit reference file etc. The DPA is not restricted to information held by/on behalf of public authorities or those bodies carry out a public function nor is its purpose limited to the right of access to information. For further information, refer to http://www.ico.gov.uk/

The Data Protection Act applies to England, Ireland, Scotland, and Wales.

There are two other accesses to information regimes, which the Scottish Information Commissioners Office has responsibility for:

- Freedom of Information (Scotland) Act 2002
- Environmental Information (Scotland) Regulations

Freedom of Information (Scotland) Act 2002
The Freedom of Information (Scotland) Act 2002 enables any person to obtain information from Scottish public authorities. This is a legal right and will ensure that all people get information to which they are entitled.

This legal right of access includes all types of recorded information of any date held by Scottish public authorities. From 1 January 2005, any person who makes a request for information must be provided within it, subject to certain conditions.

Information highlighting the legislation can be found on www.itspublicknowledge.info/legislation

Environmental Information (Scotland) Regulations
The Environmental Information (Scotland) Regulations enable people access to environmental information.

Reviewed by: Nick Clark
Last Reviewed: Nov 2025
Next Review Date: Nov 2028