NON CONFIDENTIAL

# Data Protection Policy

## 1.0 SCOPE

### 1.1 Purpose

1.1.1 The purpose of the Data Protection Policy is to ensure that:

- we meet our obligations under data protection legislation;
- appropriate technical and organisational measures are in place across the business to safeguard the rights and freedoms of individuals; and
- colleagues, contractors and suppliers are aware of their responsibilities in connection with this Policy.

1.1.2 The Policy applies to whg and all its subsidiary and associate organisations, referred to in this document as 'the Group'.

### 1.2 Legal and regulatory framework

1.2.1 The requirements relating to data protection are set out in the General Data Protection Regulation (GDPR) and the Data Protection Act 2018. We are required to safeguard the rights and freedoms of individuals when processing their personal data.

1.2.2 The Regulator of Social Housing requires registered providers to "adhere to all relevant law". This Policy is designed to ensure that we adhere to data protection legislation.

### 1.3 Roles and Responsibilities

1.3.1 whg Board carries ultimate responsibility for ensuring that we comply with legislation, in particular GDPR and data protection legislation.

1.3.2 The Board Champion is responsible for advising and assisting the Board in its overall development and knowledge on data protection and information security, providing informed challenge and enabling the Board to contribute to the debate.

1.3.3 The Data Protection Officer (DPO) is responsible for carrying out a range of statutory duties; these are summarised at Appendix 2.

1.3.4 All colleagues are responsible for data protection, as set out in section 2.3.

## 2.0 POLICY STATEMENT

### 2.1 Key principles

2.1.1 We deliver services in line with our Corporate Plan. To do this effectively, we need to collect information from potential and existing customers, job applicants and colleagues, board and committee members, grant applicants and partners, for example suppliers. Much of this information is personal data.

2.1.2 A list of **definitions** of terms associated with data protection can be found at Appendix 1.

2.1.3 Security of personal data and special categories of personal data is a priority for whg. Unauthorised disclosure will be taken seriously and may be deemed to be a disciplinary offence, depending on the materiality of the breach. This Policy applies equally to personal data held in computer records and in manual paper files.

2.1.4 We will comply with data protection legislation including the principles in Article 5 of the GDPR. These are set out in Appendix 3, together with a brief description of how we will comply with each one.

2.1.5 The GDPR and the Data Protection Act 2018 impose restrictions on the transfer of personal data outside the European Union (EU). We will not normally transfer personal data outside the EU and will not permit our data processors to do so without our agreement. When commissioning services that are processed in the Cloud, we will engage with suppliers to ensure that GDPR conditions are met and that the data cannot be compromised by a third party.

### 2.2 Governance and Accountability

2.2.1 The GDPR includes provisions that promote accountability and governance. The accountability principle in Article 5(2) requires us to demonstrate that we comply with the principles by:

- implementing appropriate technical and organisational measures that ensure and demonstrate that we comply, such as colleague training and internal audits of processing activities;
- maintaining relevant documentation on processing activities;
- appointing a DPO;
- implementing measures that meet the principles of data protection

by design and data protection by default;
- using data protection impact assessments where appropriate; and
- adhering to approved codes of conduct.

2.2.2 whg's Information Security and Data Protection Management System establishes a formal framework for the protection of personal data processed by whg. It also covers:
- the protection of our business information assets
- the management of third party processing of, or access to, personal data for which we are the data controller
- the protection of information processed on behalf of another data controller where we act as a data processor.

2.2.3 The Information Security Forum will exercise oversight and responsibility for the implementation of the framework. The DPO will maintain a register of data processing activities.

2.2.4 We will appoint a Board Champion for Data Protection and Information Security who will be invited to meetings of the Information Security Forum.

**2.3 Colleague responsibilities**

2.3.1 Colleagues must keep personal data secure. Access to systems and information, whether manual or computerised, will be restricted to the appropriate colleagues according to their role through a defined role based access procedure. Colleagues must access personal data only where they need it to carry out their job and there is a business need to do so. Accessing data for personal gain/interest is a disciplinary offence which could lead to sanctions up to and including dismissal.

2.3.2 All colleagues have a responsibility to comply with data protection principles. They must follow the guidance published on the colleague intranet, including :
- keep hard copy files and information locked away when not in use
- never share a password with anyone else
- always lock computer screens when away from the desk
- be careful to send emails, letters and attachments to the correct person
- keep papers and all devices secure when out of the office; do not leave them in a vehicle overnight
- only use data for the purpose it was collected
- update, destroy or delete data when it is out of date or no longer required (unless there is a legal requirement to keep it)
- never share any personal data over the phone or in any other way (including email) unless you are absolutely sure who you are giving it to and that they are entitled to that information.

2.3.3 All colleagues will receive mandatory annual training to ensure that they understand their responsibilities for data protection and cyber security. Records of the training will be kept as evidence of whg's compliance with legal requirements.

2.3.4 Colleagues will follow the Information Commissioner's Office (ICO) Codes of Practice where appropriate including:

- Data Sharing Code of Practice
- CCTV Code of Practice
- Conducting Privacy Impact Assessments Code of Practice

## 2.4 Data Security Breaches

2.4.1 Data will be processed in line with the Information Security Policy. Any colleague discovering a breach of information or data security must inform their line manager and the appropriate colleague according to the type of breach. All such breaches will be handled in line with our Information Security Breach Procedure.

2.4.2 The DPO must be informed as soon as possible if the breach involves personal data. The DPO will decide, in conjunction with the Corporate Director of Governance and Compliance, whether the breach must be reported to the ICO and to the data subjects themselves. Any breaches that need to be reported to the ICO must be reported with 72 hours of discovering the breach. Breaches, including any that are reported to the ICO will be reported to GEXEC.

2.4.3 The DPO will keep records of breaches and near misses. Trends and lessons learnt will be reported to the Information Security Forum.

## 2.5 Data retention

2.5.1 The data protection principles require that personal data should not be kept for longer than required and that it should be kept up to date.

2.5.2 Colleagues will ensure that information is kept up to date, as far as is reasonably practicable. Information that is no longer necessary must be destroyed or deleted in line with the Data Retention Policy. However, care should be taken not to delete information before the statutory minimum retention periods for specific types of documents and records. These can be found in the National Housing Federation's (NHF) Document Retention Guidelines as revised by whg.

## 2.6 Data Subject Rights

2.6.1 The Data Protection Act gives rights to individuals in respect of the

personal data that we hold about them. These are:

- the right to be informed
- the right of access
- the right to rectification
- the right to erasure
- the right to restrict processing
- the right to data portability
- the right to object to processing
- the right to object to automated decision making and profiling and
- the right to claim compensation for damages caused by a breach of the Act.

2.6.2 We will give individuals access to their personal records in accordance with the Data Protection Act and whg's Data Subject Access Request procedures. The DPO will deal with and keep records of all such requests. Requests will be dealt with within one calendar month in line with the data subject rights process.

2.6.3 Our Privacy Notices set out the rights of individuals. These include Privacy Notices for customers, colleagues and applicants for grants or to join our Boards or Committees.

**2.7 Data Protection Officer (DPO)**

2.7.1 We will appoint an appropriately experienced and qualified DPO to ensure compliance, and to advise on any Data Protection Issues. The role of the DPO will be in line with the requirements of the GDPR and is summarised in Appendix 2.

2.7.2 The DPO will keep the ICO's registrations for the Group up to date.

**2.8 Privacy by Design**

2.8.1 We have an obligation to implement technical and organisational measures to show that we have considered and integrated data protection into our processing activities. This is known as 'Privacy by Design'.

2.8.2 Privacy by Design means that data protection must be considered formally in the early stages of projects, for example when:

- procuring new IT systems for storing or accessing personal data;
- developing policies or strategies that have privacy implications;
- embarking on a data sharing initiative;

- using data for new purposes; or
- collecting new personal data.

2.8.3 This is done by carrying out a data protection impact assessment (DPIA). Colleagues must consult the DPO, who will work with teams to conduct a pre-screening assessment. The DPO will advise colleagues where a full DPIA is required and support them to complete it.

**2.9 Contracts and procurement**

2.9.1 Data protection must be considered formally as part of the engagement of new third party suppliers. Colleagues must consult Procurement and the DPO, who will work with teams to conduct a pre-screening assessment. The DPO will advise colleagues where a full DPIA is required and support them to complete it.

2.9.2 We will require our contractors and suppliers to enter into a contract containing a data protection clause and setting out their responsibilities as a data processor where appropriate.

**2.10 Data Processors**

2.10.1 It is a legal requirement that Data Processors must be appointed by contract. The contract will stipulate that:

- the contractor/supplier warrants that it will act only on whg's instructions and
- will provide security guarantees that appropriate security measures must be taken against unauthorised/unlawful access and accidental loss or destruction of the data.

2.10.2 whg will use secure methods of sending data to our Data Processors, for example secure file transfer protocols. Data Processors will be instructed to destroy personal data at the end of the contract.

**2.11 Data Sharing**

2.11.1 Data protection legislation requires that personal data must be shared in line with certain conditions. Data sharing agreements will be put in place to set out the conditions for regular data sharing with our partners where appropriate.

2.11.2 Colleagues must consult the DPO if we receive a request for disclosure of personal data that is outside the terms of a data sharing agreement. The DPO will keep records of disclosure requests.

2.11.3 Data sharing with our data processors will take place in line with the

contract.

**2.12 Audit and compliance monitoring**

2.12.1 A programme of internal compliance audits and checks will be carried out to ensure that we are complying with our own policies. This process will be overseen by the Information Security Forum.

## 3.0 PERFORMANCE MEASURES

3.1 We will renew the annual registration of the relevant members of the Group as required within the Information Commissioner's deadlines.

3.2 We will respond to Data Subject Access Requests within one calendar month.

3.3 The Information Security Forum will monitor:

- the number and type of data security breaches
- turnaround times for subject access requests
- delivery of the risk treatment plan and
- delivery of actions arising from information governance audits

## 4.0 TRAINING AND DISSEMINATION

4.1 All colleagues need to be aware of this Policy. They will be informed about the Policy during briefings, face to face training, compliance reviews and whoogle reminders as well as the annual mandatory training.

## 5.0 MONITOR AND REVIEW

5.1 This Policy will be monitored by the Corporate Director of Governance and Compliance and reviewed every three years by the Policy Group, Information Security Forum and whg Board.

## 6.0 ASSOCIATED DOCUMENTS, POLICIES AND PROCEDURES

6.1 General Data Protection Regulation and Data Protection Act 2018 and associated guidance

Information Security Policy
Electronic Devices Acceptable Usage Policy
Data Retention Policy
Data Subject Rights Procedure
Information Security Breach Procedure
Colleague Code of Conduct

Board and Committee Member Code of Conduct
Colleague and Customer Privacy Notices
Information Security and Data Protection Management System

NON CONFIDENTIAL

APPENDIX 1

## Definitions

**Data controller** means an organisation or person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed. whg is a data controller.

**Data processor**, in relation to personal data, means any organisation or person (other than an employee of the data controller) who processes the data on behalf of the data controller. For example, the company that sends out rent account letters on whg's behalf is a data processor.

**Data subject** means an individual who is the subject of personal data. whg's customers, applicants, colleagues and participants in projects are all data subjects.

**Personal data** refers to personal information relating to the person who supplies it or to another individual, for example household members. It refers to any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier.

**Processing**, in relation to information or data, means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

(a) organisation, adaptation or alteration of the information or data,

(b) retrieval, consultation or use of the information or data,

(c) disclosure of the information or data by transmission, dissemination or otherwise making available, or

(d) alignment, combination, blocking, erasure or destruction of the information or data.

**Sensitive / special categories of personal data** means personal data consisting of information regarding:

(a) racial or ethnic origin

(b) political opinions,

(c ) religious or philosophical beliefs

(d) trade union membership

(e) data concerning health

(f) sex life or sexual orientation

(g) genetic or biometric data

## APPENDIX 2

### Role of the Data Protection Officer

At whg, the statutory DPO role is part of the Data Governance Officer's job.

**1.** The DPO's role, as set out in the General Data Protection Regulation, is:

- to inform and advise the organisation and its colleagues about their obligations to comply with the GDPR and other data protection laws
- To monitor compliance with the GDPR and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train colleagues and conduct internal audits.
- To be the first point of contact for supervisory authorities and for individuals whose data is processed (colleagues, customers etc).

**2.** The DPO will be involved in all issues relating to data protection, in particular in carrying out data protection impact assessments, checking the compliance of data processing activities and issuing recommendations to the data controller.

**3.** The DPO must be informed promptly when a data breach occurs. In his/her absence, the Corporate Director of Governance and Compliance must be informed.

**4.** The DPO will perform his/her tasks in an independent manner and will report to the Company Secretary. He/she will provide reports to the Board from time to time.

**5.** The DPO will have the power to veto or suspend the processing of personal data if he/she believes that it is unlawful. He/she also has the power to make the decision to report a breach to the ICO. This will usually be done in consultation with the Corporate Director of Governance and Compliance. Breaches will be reported by the DPO to GEXEC.

## APPENDIX 3

### Special category and criminal offence personal data processed in line with Schedule 1 of the Data Protection Act 2018

This appendix explains how we comply with the principles in GDPR Article 5 and our policies as regards retention and erasure.

| A | Compliance with Article 5 Principles: |
|---|---|
| | |
| **1.** | Personal data shall be: |
| 1.1 | **processed lawfully, fairly and in a transparent manner in relation to individuals:** we have Privacy Notices to inform customers and colleagues what personal data we process, what we do with it, who we share it with and the lawful grounds for processing. Our data protection and information security policies and management framework will ensure that data protection and information security are managed effectively across the organisation. |
| | |
| 1.2 | **collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes:** whg's Privacy Notices inform data subjects of the purposes for processing their personal data and we maintain a register of processing activities. |
| | |
| 1.3 | **adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed:** our policy is to collect only the data that is necessary and to restrict access to information to those colleagues that need it to do their job. |
| | |
| 1.4 | **accurate and where necessary kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay:** our Data Subject Rights Process sets out how we will deal with requests for erasure and rectification. We provide an on-line facility for customers to update their own details and take appropriate steps to keep data up to date. |
| | |
| 1.5 | **kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed:** we keep personal data in line with our retention schedule and will undertake cleansing of our data. We will introduce automated deletion or anonymisation of data where possible. |

| | |
|---|---|
| | |
| | |
| 1.6 | **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:** all our colleagues receive mandatory annual training on data protection and we have a robust data security breach reporting procedure. The Data Protection Officer monitors data breach and near miss trends and shares lessons learnt with colleagues. Appropriate cyber security measures are in place and we continue to learn from good practice across the sector. |
| | |
| **B** | **Policies relating to retention and erasure** |
| | |
| 1.7 | whg will use reasonable endeavours to ensure that data is kept no longer than necessary and will retain the data required to carry out our legal obligations and provide services to our customers. |
| | |
| 1.8 | Data that is no longer necessary will be destroyed or deleted in line with the Disposal and Retention Considerations and the NHF Document Retention Schedule as revised by whg. Colleagues will ensure that data is kept up to date, as far as is reasonably practicable. |
| | |
| 1.9 | If a request is received for the erasure of special category or criminal offence personal data, it will be dealt with by the Data Governance Officer. The request will be reviewed to ensure it complies with one or more of the grounds for erasure:<br><br>• The data subject has withdrawn consent on which the processing is based and there are no overriding legitimate grounds for the processing;<br>• The personal data has been unlawfully processed; or<br>• The personal data must be erased for compliance with a legal obligation.<br><br>If the request complies with one of the above, it will be erased within 30 days of the request being received. Other requests will be considered individually by the Data Governance Officer. |
| | |
| 1.10 | All personal data will be kept in line with the NHF Document Retention Schedule as revised by whg. In general it will be kept as follows:<br><br>• **Colleague data**<br>  ○ For the duration of employment with whg and for six years after the colleague has left<br>  ○ Six years after employment ceases for accident and sickness records<br>• The exception to the retention period for colleagues is:<br>  ○ 40 years for medical records relating to asbestos |

| | |
|---|---|
| | • **Customer Data**<br>  ○ Data relating to the tenancy will be kept for the length of the tenancy and an additional six years<br>  ○ Warning markers and records of violent behaviour are kept for the length of the tenancy<br>  ○ Records relating to offenders, ex-offenders and persons subject to cautions will be kept for the length of the tenancy plus six years,<br><br>The exceptions to the retention period for customers are as follows:<br>• We will keep a record that the individual was once our customer and the amount of outstanding debt if there is any;<br>• Some records of violent behaviour and/or ongoing cases will need to be kept after the end of the tenancy in order to deliver the Restricted Access Policy;<br>• We will keep data about offences committed by non-whg customers whose details we receive via multi-agency partnerships and the police for the length of the licence (which could vary). |

| | |
|---|---|
| **Document author** | Helen Lane, Data Governance Officer |
| **Document owner** | Corporate Director of Governance and Compliance |
| **Legal advice** | Advice provided by Data Protection consultant and our solicitors |
| **Consultation** | Information Security Forum |
| **Approved by** | Information Security Forum December 2019<br>Policy Group December 2019<br>whg Board January 2020 |
| **Review Date** | July 2023 |
| **Corporate Plan aim** | • Deliver a strong business, fit for today and prepared for tomorrow |
| **Equality analysis** | Not applicable |
| **Key changes made** | Policy revised to incorporate key points from the Cyber Security Policy and update terminology. Section added about training and dissemination.<br>Appendix 3 has been updated in line with the advice provided by Anthony Collins Solicitors at a recent briefing. |