Data Protection Policy

1.0	**SCOPE**
1.1	**Introduction**
	whg takes its responsibilities regarding safely accessing, holding and protecting personal information seriously and makes all efforts to abide by the requirements of the Data Protection Act 2018 (DPA), UK General Data Protection Regulation 2021("UK GDPR"), Privacy and Electronic Communications Regulations 2003 ("PECR)". This policy sets out how whg manages those responsibilities. The policy applies to all personal data processed by whg regardless of the location where that personal data is stored and regardless of the data subject. All colleagues and others processing personal data on whg's behalf must read this policy. A deliberate failure to comply with this policy may result in disciplinary action. whg's Data Protection Officer (DPO) is Sofia Ali. She can be reached at DataProtection@whgrp.co.uk Note that should the DPO be unavailable, the Data Governance Officer can assist in their absence.
1.2	**Purpose**
	This document sets out whg's policy to ensure: 1. clarity about how personal data must be processed and whg's expectations for all those who process personal data on its behalf; 2. compliance with the data protection law and with good practice; and 3. protection of whg's reputation by ensuring personal data is processed in accordance with data subjects' rights.
1.3	**Legal and regulatory framework**
	The DPA and UK GDPR set out the requirements relating to Data Protection. whg has a duty to safeguard the rights and freedoms of individuals when processing their Personal and Sensitive Data. The Information Commissioner's Office oversees compliance with these requirements. The Regulator of Social Housing requires registered providers to "adhere to all relevant Law".
2.0	**POLICY STATEMENT**
2.1	whg is committed to compliance with all relevant Data Protection legislation and the protection of the "rights and freedoms" of individuals whose information whg collects and processes in accordance with the DPA and UK GDPR. whg is also committed to protecting and respecting personal data, being transparent on how whg processes personal data, and demonstrating accountability in handling data.

3.0	**POLICY DETAILS**
3.1	**Personal data protection principles**
	Those principles set out in the DPA and UK GDPR require personal data to be: 1. processed lawfully, fairly and in a transparent manner; 2. collected only for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes; 3. adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed; 4. accurate and where necessary kept up to date; 5. not kept in a form which permits identification of data subjects for longer than is necessary for the purposes for which the personal data is processed; and 6. processed in a manner that ensures its security, using appropriate technical and organisational measures to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.
3.2	**Data Subject Rights**
	Data subjects have rights in relation to the way whg handles their personal and sensitive data. These include the following rights: 1. where the legal basis of processing is Consent, to withdraw that Consent at any time; 2. to ask for access to the personal data that whg holds (see below); 3. to prevent use of the personal data for direct marketing purposes; 4. to object to processing of personal data in limited circumstances; 5. to ask whg to erase personal data without delay: a. if it is no longer necessary in relation to the purposes for which it was collected or otherwise processed; b. if the only legal basis of processing is consent and that consent has been withdrawn and there is no other legal basis by which whg can process that personal data; c. if the data subject objects to processing where the legal basis is the pursuit of a legitimate interest or the public interest and whg can show no overriding legitimate grounds or interest; d. if the data subject has objected to processing for direct marketing purposes; e. or if the processing is unlawful. 6. to ask whg to rectify inaccurate data or to complete incomplete data; 7. to restrict processing in specific circumstances e.g. where there is a complaint about accuracy; 8. to ask whg for a copy of the safeguards under which personal data is transferred outside of the EU; 9. the right not to be subject to decisions based solely on automated processing, including profiling, except where necessary for entering into, or performing, a contract, with whg; it is based on the data subject's explicit consent and is subject to safeguards; or is authorised by law and is also subject to safeguards; 10. to prevent processing that is likely to cause damage or distress to the data subject or anyone else; 11. to be notified of a personal data breach which is likely to result in high risk to rights and freedoms; 12. to make a complaint to the ICO.

3.3	**Data Subject Access Requests**
	Data subjects have the right to receive a copy of their personal data which is held by whg. In addition, an individual is entitled to receive further information about whg's processing of their personal data which includes: 1. the purpose; 2. the categories of personal data being processed; 3. recipients/categories of recipient; 4. retention periods; 5. information about data subject's rights; 6. the right to complain to the ICO; 7. details of the relevant safeguards where personal data is transferred outside the EEA; and 8. any third-party source of the personal data. whg colleagues should not allow external third parties to persuade them into disclosing personal data about customers or colleagues without proper authorisation and agreement from the Data Protection Officer. Colleagues must not alter, conceal, block or destroy personal data once a request for access has been made. Colleagues must contact the Data Protection team for all subject access requests.
3.4	**Accountability**
	whg is responsible for, and must be able to demonstrate compliance with, the data protection principles, applying adequate controls including: 1. appointing a suitably qualified DPO; 2. implementing Privacy by Design when processing personal data and completing a Data Protection Impact Assessment (DPIA) as required; 3. integrating data protection into policies and procedures, in the way personal data is handled and by producing required documentation such as Privacy Notices, Records of Processing Activities, and records of Personal Data Breaches; 4. training colleagues on compliance with Data Protection Law and keeping appropriate training records; and 5. regularly testing the measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.
3.5	**Responsibilities**
3.5.1	whg responsibilities - as the Data Controller, whg is responsible for establishing policies and procedures in order to comply with data protection law.
3.5.2	Data Protection Officer responsibilities - DPO is responsible for: 1. advising whg colleagues of obligations under DPA and UK GDPR; 2. monitoring compliance with relevant data protection law, and ensuring relevant policies are in place; 3. delivering training and awareness sessions and ensuring up to date training compliance; 4. providing advice where requested on data protection impact assessments;

	5. cooperating with and acting as the contact point for the Information Commissioner's Office; and 6. assessing risk associated with processing operations, considering the nature, scope, context and purposes of processing
3.5.3	Colleagues' responsibilities - colleagues must ensure that: 1. all personal data is kept securely; 2. no personal data is disclosed either verbally or in writing, accidentally or otherwise, to any unauthorised third party; 3. personal data is kept in accordance with whg's retention schedule; 4. any queries regarding data protection, including subject access requests and complaints, are promptly directed to the Data Protection team; 5. any data protection breaches are swiftly brought to the attention of the Data Protection Officer and/or Data Governance Officer and that they support the Data Protection team in resolving breaches; and 6. where there is uncertainty around a data protection matter advice should be sought from the Data Protection Officer or the Data Governance Officer.
3.6	**Reporting a Personal Data Breach**
	The DPA and UK GDPR requires organisations to report to the Information Commissioner's Office (ICO) any personal data breach where there is a risk to the rights and freedoms of the data subject. Where the personal data breach results in a high risk to the data subject, they also have to be notified unless subsequent steps have been taken to ensure that the risk is unlikely to materialise, security measures were applied to render the personal data unintelligible (e.g. encryption) or it would amount to disproportionate effort to inform the data subject directly. whg have put in place procedures to deal with any suspected personal data breach and will notify data subjects or the ICO where legally required to do so. If a colleague knows or suspects that a personal data breach has occurred, they should immediately contact the Data Protection Officer and Data Governance Officer at DataProtection@whgrp.co.uk and follow the instructions in the personal data breach procedure. All evidence relating to personal data breaches must be retained to maintain a record of such breaches, as required by the DPA and UK GDPR.
3.7	**Third-Party Data Processors**
	Where external companies are used to process personal data on behalf of whg, responsibility for the security and appropriate use of that data remains with whg. Where a third-party data processor is used: 1. a data processor must be chosen which provides enough guarantees about its security measures to protect the processing of personal data; 2. reasonable steps must be taken that such security measures are in place; 3. a written contract establishing what personal data will be processed and for what purpose must be set out; and 4. a data processing agreement, available from the Data Protection Team, must be signed by both parties.

	For further guidance about the use of third-party data processors please contact the Data Protection Team.
3.8	**Limitations on Transfer of Personal Data**
	The DPA and UK GDPR restricts data transfers to countries outside the EU in order to ensure that the level of data protection afforded to individuals by the DPA and UK GDPR is not undermined. Colleagues may only transfer personal data outside the EU with the explicit permission of the Data Protection Officer and/or Data Governance Officer.
3.9	**Record Keeping**
	The DPA and UK GDPR requires full and accurate records of all data processing activities to be maintained. The Data Protection Team keep records of the name and contact details of whg as Data Controller and the DPO, clear descriptions of the personal data types, data subject types, processing activities, processing purposes, third-party recipients of the personal data, personal data storage locations, personal data transfers, the personal data's retention period and a description of the security measures in place. Records of personal data breaches must also be kept, setting out: 1. the facts surrounding the breach; 2. its effects; and 3. the remedial action taken
3.10	**Data privacy by design and default and Data Protection Impact Assessments (DPIAs)**
	whg is required to implement privacy-by-design measures when processing personal data, by implementing appropriate technical and organisational measures (like pseudonymisation) in an effective manner, to ensure compliance with data protection principles. whg must ensure therefore that by default only personal data which is necessary for each specific purpose is processed. The obligation applies to the volume of personal data collected, the extent of the processing, the period of storage and the accessibility of the personal data. By default, personal data should not be available to an indefinite number of persons. whg must also conduct DPIAs in respect of high-risk processing before that processing is undertaken. DPIAs should be conducted and discussed with the DPO in the following circumstances: 1. use of new technologies (programs, systems or processes), or changing technologies; 2. automated processing including profiling; 3. large scale processing of personal and sensitive data; and 4. large scale, systematic monitoring of a publicly accessible area. A DPIA must include: 1. a description of the processing, its purposes and the Data Controller's legitimate interests if appropriate; 2. an assessment of the necessity and proportionality of the processing in relation to its purpose; 3. an assessment of the risk to individuals; and 4. the risk-mitigation measures in place and demonstration of compliance.

3.11	**Direct Marketing**
	whg is subject to privacy laws when marketing to customers, applicants and any other potential user of services that are not part of the housing management function. The right to object to direct marketing (not relating to tenancy/housing) must be explicitly offered to the data subject in an intelligible manner so that it is clearly distinguishable from other information. A data subject's objection to direct marketing must be dealt with promptly. If a data subject opts out at any time, their details should be updated as soon as possible.
3.12	**Sharing Personal Data with Third Parties**
	In the absence of consent, a legal obligation or other legal basis of processing, personal data should not generally be disclosed to third parties unrelated to whg (e.g. customers/colleagues' family members, members of the public, private property owners). Some bodies have a statutory power to obtain information (e.g. regulatory bodies such as Councils, Revenues and Customs, Health & Care Professions Council and government agencies such as the Child Support Agency). Any such requests should be sent to the Data Protection team at DataProtection@whgrp.co.uk. Without a warrant, the police have no automatic right of access to records of personal data, though voluntary disclosure may be permitted for the purposes of preventing/detecting crime or for apprehending offenders. Any request for information should be sent to the Data Protection team at DataProtection@whgrp.co.uk. In certain situations, sharing of personal data for research purposes may also be permissible, subject to certain safeguards and subject to the approval of the Data Protection Officer and/or Data Governance Officer.
4.0	**PERFORMANCE MEASURES**
4.1	• Annual registration of whg and trading Companies will be renewed as required by the Information Commissioner's deadlines. • Subject access requests to be responded to within one calendar month. • Data security breaches will be investigated and reported with 72 hours. • Monitoring the delivery of the risk treatment plan and actions arising from information governance audits. • The DPO will ensure that all colleagues are provided training to ensure compliance with the Data Protection Law and that compliance with training required by whg is monitored. • An annual assurance report will be provided to the Audit and Assurance Committee.
5.0	**EQUALITY AND DIVERSITY**
5.1	This Policy applies to all whg colleagues, Board and Committee Members, volunteers, contractors and agents and other relevant third parties who may have access to or use of whg related data.

6.0	**TRAINING AND DISSEMINATION**
6.1	All whg colleagues undergo adequate training to enable them to comply with Data Protection Law including mandatory data privacy related training via noodle and face to face training delivered by the Data Protection team.
7.0	**MONITOR AND REVIEW**
7.1	This Policy will be monitored by the Corporate Director of Governance and Compliance and reviewed every three years by the Policy Group and approved by the whg Board.
8.0	**ASSOCIATED DOCUMENTS, POLICIES AND PROCEDURES**
8.1	Documents, policies and procedures associated with this Policy are: 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

Document author	Data Protection Officer
Document owner	Corporate Director of Governance and Compliance
Legal advice	Data Protection Officer
Consultation	N/A
Approved by	Approved by Policy Group July 2023 Approved by whg Board July 2023
Review Date	July 2024
Corporate Plan aim	Deliver a strong business, fit for today and prepared for tomorrow
Equality Assessment	N/A
Key changes made	Policy updated in line with the DPA 2018 and UK GDPR 2021