Data Protection Policy

Responsible director	Shahida Latif-Haider, Executive Director – Transformation and Resources
Policy monitoring body	Strategic Information Committee (Review) Group Board (Approval)
Resident input into policy	N/A
Policy review due	April 2026
Linked strategies/policies	Data Governance Strategy Special Category Data Policy Information Sharing Policy Data Retention Policy Data Protection Impact Assessment (DPIA) Policy Data Protection Consent Policy Information Rights Policy Use of Data Processors Policy Information Security Incident Policy Information Security policies
Version	V2.6
Date of approval	24 July 2023

1. Purpose and scope

1.1. The purpose of this policy is to ensure compliance with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act (DPA) 2018 and related national legislation ('the data protection laws'). This legislation governs the storing or handling ('processing') of information ('personal data') about living identifiable individuals ('data subjects').

1.2. This policy applies to all parts of Wythenshawe Community Housing Group (WCHG – 'the Group').

1.3. This policy applies to all colleagues. In this policy, the term 'colleagues' means anyone working in any context within the Group at whatever level or grade and whether permanent, fixed term or temporary, including but not limited to employees, trainees, interns, seconded colleagues, agency colleagues, agents, volunteers, board members and external members of committees.

1.4. This policy is not, and should not be confused with, a privacy notice (a statement informing data subjects how their personal data is used by the Group). The Group's Privacy Notice is currently available on the internet, in layered and summary versions, at www.wchg.org.uk/privacy-notice.

1.5. This policy should be read in conjunction with the following documents, which supplement this policy where applicable:

1.5.1. information security policies, procedures and terms and conditions, which concern the confidentiality, integrity and availability of Group information, and which include rules about acceptable use, incident management and reporting, IT monitoring, and the use of personal mobile devices;

1.5.2. information sharing policy and guidance;

1.5.3. colleague employment contracts and comparable documents (e.g. volunteer agreements), which are owed a duty of confidence by the Group;

1.5.4. records management policies and guidance, which govern the appropriate retention and destruction of Group information; and

1.5.5. any other contractual obligations on the Group or individual colleagues which govern the management of information held by the Group, which

may require us to comply with other regulations (e.g. security requirements for funded programmes).

2. Policy statement

2.1. The Group will support and uphold the information rights of our customers and colleagues. This policy sets out how we will do this by enabling our colleagues to comply with the data protection laws as part of their everyday working practices.

2.2. 'Complying with the data protection laws' may be summarised as but is not limited to:

2.2.1. applying the data protection principles when processing personal data;

2.2.2. fulfilling the rights given to data subjects under the data protection laws; and

2.2.3. implementing the Group's accountability and transparency obligations under the data protection laws.

2.3. The Group is committed to the principle of privacy by design. Measures that the Group will take include, but are not limited to:

2.3.1. adopting a 'privacy first' approach when creating new applications, processes and developing new systems;

2.3.2. ensuring that data protection and privacy issues are considered for all systems, strategies, policies, and procedures;

2.3.3. ensuring that data protection and privacy issues are considered in formal papers to the Board, Group Leadership Team (GLT) and relevant Committees and working groups.

3. Roles and responsibilities

3.1. The Group has a corporate responsibility as a data controller (or when acting as a joint data controller or a data processor) for:

3.1.1. complying with the data protection laws and holding records demonstrating this;

3.1.2. cooperating with the Information Commissioner's Office (ICO) as the UK supervisory authority for the data protection laws; and

3.1.3. responding to regulatory/court action and paying administrative levies and fines issued by the ICO.

3.2. The Board is responsible for:

3.2.1. reviewing and approving this policy and ensuring appropriate resources and processes are in place and implemented to enable compliance with the data protection laws.

3.3. Group Audit & Risk Committee (GA&RC) is responsible for:

3.3.1. reviewing the overall information risk profile;

3.3.2. receiving and reviewing the reports of the Group Data Protection Officer (DPO) and the Strategic Information Committee (SIC), including details of information security incidents such as data breaches and the remedial actions taken to reduce risk; and

3.3.3. reporting any concerns about unacceptable levels of information risk to Board.

3.4. GLT is responsible for:

3.4.1. ensuring that the data protection laws and the data protection principles which underpin them, are followed across the organisation;

3.4.2. ensuring that Data Ambassadors are recruited and supported in each area of the business, to increase colleagues' confidence that they are using and applying personal data appropriately;

3.4.3. ensuring that data-driven projects, and other systems and processes designed and implemented by the Group, include data protection by design and default; and

3.4.4. receiving and reviewing the reports of the SIC to have regular oversight of patterns and trends of information risk.

3.5. The Group DPO is responsible for:

3.5.1. adopting a risk-based approach in relation to data processing;

3.5.2. informing and advising the Group on all aspects of its compliance with the data protection laws;

3.5.3. monitoring the Group's compliance with the data protection laws and with the Group's own data protection policies. This may involve:

- Assigning responsibilities;
- Awareness-raising initiatives;
- Training of colleagues involved in data processing;
- Audits relating to data processing.

3.5.4. providing advice, where requested, on Data Protection Impact Assessments (DPIAs) and monitoring their compliance with Article 35 of the UK GDPR;

3.5.5. acting as the Group's standard point of contact with the ICO with regard to the data protection laws. This includes potential and actual breaches of the data protection principles, where they believe the rights and freedoms of customers or colleagues may have been harmed; and

3.5.6. providing an independent point of contact for customers and colleagues to raise any issues related to processing of their personal data and to the exercising of their rights under the data protection laws. This includes investigating complaints about any restrictions of these rights, and carrying out or commissioning internal reviews into the way the Group handled their data.

3.6. The Information Governance (IG) team, in collaboration with other relevant colleagues, is responsible for:

3.6.1. providing advice, guidance, training and tools/methods (including annual mandatory training for all colleagues), in accordance with the Group's overall risk profile, relevant case law and ICO/other regulatory guidance, to help teams and colleagues comply with this policy;

3.6.2. publishing and maintaining this Policy, the Group privacy notice, and supporting the management of other Group-wide data protection documents including the Group's Records of Processing Activities (ROPA), Information Asset Register (IAR) and DPIAs;

3.6.3. advising on the completion of DPIAs and other privacy products, handling data protection rights requests, advising on appropriate disclosures of data under the data protection laws (such as the appropriate use of consent set out in the Group's Data Protection

Consent and Special Category Data policies), and investigating personal data breaches;

3.6.4. providing training and support to Information Asset Owners, Data Ambassadors and their wider teams, to improve their confidence in applying the data protection principles in their everyday practice; and

3.6.5. highlighting high risks to individual rights and freedoms identified in information security incident investigations, DPIAs and other data risk assessment processes, ensuring that managers and leaders have oversight of these risks so they can mitigate them appropriately.

3.7. Managers and Leaders are responsible for:

3.7.1. making all colleagues within their department aware of this policy as necessary, and ensuring that their colleagues have completed mandatory data protection training which enables them to abide by this policy;

3.7.2. ensuring that appropriate processes, guidance and bespoke training are implemented within their department to enable compliance with the data protection laws;

3.7.3. ensuring that they have sufficient Data Ambassadors in their department and working with them to manage the data processing risks associated with their projects and services;

3.7.4. ensuring that appropriate arrangements are in place with all instances of outsourced processing (eg. the supply of personal data to contractors) and/or data sharing;

3.7.5. ensuring that DPIAs are carried out for high risk processing activities, working with the IG team to identify appropriate controls to reduce these risks to an acceptable level, and accepting the residual risk;

3.7.6. with the IG team's advice and support, creating privacy statements for projects and services which collect personal data, and that where these collection processes are routine, reviewing these statements annually;

3.7.7. liaising with the IG team where personal data collection forms may need to be designed or improved to meet the requirements of the data protection laws. This includes how consents are managed and documents are stored so that data subjects can exercise their information rights;

3.7.8. owning the information assets within their department, managing the risks associated with those assets and including the information assets within their team in the Group's Information Asset Register;

3.7.9. ensuring that data processing activities processes within their department are updated in the ROPA, including purposes of processing, any third party disclosures or international transfers, and other information required under the data protection laws;

3.7.10. monitoring patterns and trends of information risk in their area, attending the SIC on a quarterly basis to report, consider and tackle these risks holistically;

3.7.11. recognising and reporting information security incidents such as personal data breaches to the IG team, and cooperating with any corrective actions arising from their investigation of these incidents; and

3.7.12. recognising, reporting to the IG team, and cooperating with the fulfilment of data subject rights requests.

3.8. Data Ambassadors, as appropriate for their role, where identified by their Information Asset Owner and Manager, and having been provided with sufficient training and support by the IG team, are responsible for:

3.8.1. championing the aims and activities of the Data Ambassadors' network within the business areas they represent;

3.8.2. sharing communication and information across the network;

3.8.3. relaying information and/or decisions that affect business areas back to teams/departments;

3.8.4. helping the IG team to develop a flexible, interactive online presence that informs and supports their teams;

3.8.5. supporting Business Transformation projects as and when relevant;

3.8.6. understanding, recording, monitoring and reporting on the data held within areas/teams/departments;

3.8.7. identifying areas of strengths and areas for improvement in their team's data protection practice, supporting colleagues to become data confident;

3.8.8. challenging the inappropriate use of data (such as obtaining consents where systems are not in place to manage these consents), and encouraging good practice in line with data protection principles;

3.8.9. increasing data awareness and knowledge by sharing knowledge with team members and the wider Group; and

3.8.10. attending network meetings as and when possible.

3.9. Individual colleagues, as appropriate for their role and in order to enable the Group to comply with the data protection laws, are responsible for:

3.9.1. completing relevant data protection training, including an annual refresher of the GDPR e-learning module and regular Cyber awareness videos and tests;

3.9.2. following relevant advice, guidance and tools/methods depending on their role;

3.9.3. being willing to carry out the Data Ambassador role with sufficient training and support, where it is deemed appropriate and requested by the Information Asset Owner and their manager;

3.9.4. when processing personal data on behalf of the Group, only using it as necessary for their contractual duties and/or other Group roles and not disclosing it unnecessarily or inappropriately;

3.9.5. recognising and reporting information security incidents such as personal data breaches to the IG team, and cooperating with any corrective actions arising from their investigation of these incidents;

3.9.6. recognising, reporting to the IG team, and cooperating with the fulfilment of data subject rights requests; and

3.9.7. not deleting, copying or removing personal data when leaving the Group.

3.10. Failing to observe these requirements may amount to a disciplinary offence, which will be dealt with under the WCHG's disciplinary policy and procedure. Significant or deliberate breaches of this policy, such as accessing customer or colleague data without authorisation or a legitimate reason to do so, may constitute gross misconduct and could lead to dismissal without notice.

3.11. The roles and responsibilities in this policy do not waive any personal liability for individual criminal offences for the wilful misuse of personal data under the data protection laws.

4. Lawful bases for processing personal data

4.1 WCHG can only process personal data where there is a lawful basis for doing so.

4.2 The majority of personal data that the Group processes relates to customers and residents. There are a number of lawful bases that WCHG can rely upon, however in most circumstances WCHG rely on the following lawful bases (dependent on the circumstances):

- WCHG process customers' personal data 'for the purposes of legitimate interests' of providing and maintaining our properties.
- Where WCHG have a contract with our customers, personal data is processed to fulfil it.

4.3 The different requirements for the processing of special categories of personal data (as defined in Article 9 of the UK GDPR) means that 'legitimate interests' cannot be used as the sole lawful basis and there must an additional lawful basis.

4.4 WCHG therefore usually use the following additional lawful bases for special categories dependent on the processing requirement:

- In order to provide some of our services we need explicit consent by the resident. (It should be recognised that if consent was withdrawn the customer would exclude themselves from those services.) This is explained in more detail in our Data Protection Consent Policy.
- In order to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving consent.
- For completion of statutory and regulatory returns, our lawful basis is "statistical purposes in accordance … with Member State law".

5. Data Subjects' rights

5.1 WCHG recognises that data subjects have the right to:

5.1.1. be informed about the collection and use of their personal data;
5.1.2. be provided with information held about them (subject to certain exemptions set out in data protection law);
5.1.3. have incorrect or incomplete information rectified;
5.1.4. have their personal data erased (where appropriate);
5.1.5. have processing of their personal data restricted in certain circumstances;
5.1.6. have their personal data provided in a readable format and portable to another organisation, where reasonable and appropriate;
5.1.7. object to processing, including marketing, automated decisions and profiling.

5.2. WCHG believes that the personal information we hold and share belongs to the data subject and the Group will protect their information rights by constantly increasing individual choice and control.

5.3. These rights and how we ensure that our customers and colleagues can exercise control over their data, are covered in more detail in the Group's Information Rights Policy.

6. Related policies & guidance

6.1. Colleagues should contact the IG Team via their Helpdesk form on the intranet for advice and guidance on any of the requirements set out in this policy.

7. Equality and Diversity

7.1. WCHG recognises that colleagues of all races, ages, religions, gender, sexual orientation, literacy levels and disability should be treated equally and fairly. We will make every reasonable effort to ensure that no-one is discriminated against directly or indirectly on the basis of any protected characteristic as defined by the Equality Act 2010. We recognise that some protected groups may be disproportionately impacted and will take additional steps in the application of this policy and make reasonable adjustments to ensure compliance with the Act. A full Equality Impact Assessment was not found necessary for this policy.

7.2. WCHG will provide information in languages other than English, in Braille, Large Print and Audiotape where required. Our receptions and interview rooms are fitted with a hearing loop system.

7.3. If you require assistance with translation of this policy, large print, easy read, braille, or an audio copy, contact us by phone on: 0300 111 0000 or: 0800 633 5500 or by email: inclusionanddiversity@wchg.org.uk