WCHG
Data Protection Policy

Policy Name:	Data Protection Policy
Status:	Version 2.0
Approved by:	Group Board
Drafted by:	Jamie Burton
Date approved:	24 May 2018
Date effective from:	25 May 2018
E&D impact assessed:	N/A
Customer consultation:	N/A
Next Review Date:	May 2019

1. Purpose and scope

1.1. The purpose of this policy is to ensure compliance with the General Data Protection Regulation and related EU and national legislation ('data protection law'). Data protection law applies to 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 ('the Group').

1.3. This policy applies to all staff. In this policy, the term 'staff' 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 staff, agency staff, 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).

1.5. This policy should be read in conjunction with the obligations in 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. data sharing policy and guidance;

1.5.3. staff employment contracts and comparable documents (e.g. volunteer agreements), which impose confidentiality obligations in respect of information held 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 staff which impose confidentiality or data management obligations in respect of information held by the Group, which may at times exceed the obligations of this and/or other policies in specific ways (e.g. security requirements for funded programmes).

2. Policy statement

2.1. The Group is committed to complying with data protection law as part of everyday working practices.

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

2.2.1. understanding, and applying as necessary, the data protection principles when processing personal data;

2.2.2. understanding, and fulfilling as necessary, the rights given to data subjects under data protection law;

2.2.3. understanding, and implementing as necessary, the Group's accountability and transparency obligations under data protection law.

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

2.3.2. ensuring that data protection and privacy issues are considered for all formal papers to the Board, Committees and Group Leadership Team.

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 data protection law and holding records demonstrating this;

3.1.2. cooperating with the Information Commissioner's Office (ICO) as the UK regulator of data protection law; 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 (at least once a year) and approving this policy; and

3.2.2. assessing the overall risk profile and ensuring appropriate resources and processes are in place and implemented to enable compliance with data protection law.

3.3. The Executive is responsible for:

3.3.1. ensuring that data protection law and best practice is considered across the organisation;

3.3.2. ensuring that data protection within their departments is implemented effectively;

3.3.3. ensuring that systems and processes designed and implemented within their departments consider privacy by design issues.

3.4. The Group Data Protection Officer is responsible for:

3.4.1. monitoring and auditing the Group's compliance with data protection law;

3.4.2. advising the Group on all aspects of its compliance with data protection law (including its use of Data Protection Impact Assessments);

3.4.3. acting as the Group's standard point of contact with the ICO with regard to data protection law, including in the case of personal data breaches; and

3.5. The Information Management Team, in collaboration with other relevant staff, is responsible for:

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

3.5.2. publishing and maintaining core privacy notices and other Group-wide data protection documents;

3.5.3. advising on data subject rights requests; and

3.5.4. advising on Data Protection Impact Assessments, data subject complaints and personal data breaches.

3.6. Assistant Directors are responsible for:

3.6.1. making all staff within their Department aware of this policy as necessary;

3.6.2. ensuring that appropriate processes and training are implemented within their Department to enable compliance with data protection law;

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

3.6.4. ensuring that Data Protection Impact Assessments are carried out for high risk processing activities;

3.6.5. ensuring that privacy notices are in place collecting personal data, and that these are reviewed annually;

3.6.6. ensuring that personal data collection forms meet the requirements of data protection law, are stored in an approved repository (such as the intranet) and are reviewed annually;

3.6.7. owning the information assets within their Department, and managing the risks associated with those assets;

3.6.8. ensuring that appropriate processes are implemented within their Department to enable information assets containing personal data within their Department to be included in the Group's Information Asset Register, including purposes of processing and other information required under data protection law.

3.7. Senior Managers and Managers are responsible for:

3.7.1. making all staff within their teams aware of this policy as necessary;

3.7.2. ensuring that appropriate processes are implemented within their teams to enable compliance with data protection law;

3.7.3. ensuring that their staff have completed mandatory data protection training;

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

3.7.5. ensuring that Data Protection Impact Assessments are carried out for high risk processing activities;

3.7.6. ensuring that privacy notices are in place collecting personal data, and that these are reviewed annually;

3.7.7. ensuring that personal data collection forms meet the requirements of data protection law, are stored in an approved repository (such as the intranet) and are reviewed annually;

3.7.8. owning the information assets within their teams, and managing the risks associated with those assets;

3.7.9. ensuring that appropriate processes are implemented within their teams to enable information assets containing personal data within their teams to be included in the Group's Information Asset Register, including purposes of processing and other information required under data protection law;

3.7.10. recognising, reporting internally, and cooperating with any remedial work arising from personal data breaches;

3.7.11. recognising, reporting internally, and cooperating with the fulfilment of data subject rights requests.

3.8. Individual staff, as appropriate for their role and in order to enable the Group to comply with data protection law, are responsible for:

3.8.1. completing relevant data protection training;

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

3.8.3. 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;

3.8.4. recognising, reporting internally, and cooperating with any remedial work arising from personal data breaches;

3.8.5. recognising, reporting internally, and cooperating with the fulfilment of data subject rights requests; and

3.8.6. only deleting, copying or removing personal data when leaving the Group as agreed with their Head of Department and as appropriate.

3.9. Non-observance of the responsibilities in paragraph 3.8 may result in disciplinary action.

3.10. 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 data protection law.

4. Related policies & guidance

4.1. Policies

- **Data Sharing Policy**: sets out processes and procedures that must be followed when sharing data with partners e.g. local authorities and emergency services

- **Data Retention Policy**: sets out the length of time that records and documentation should be retained

- **Information Security Policy**

- **Information Handling Policy**: outlines mandatory controls for staff when handling personal or sensitive information

- **Information Security Incident Policy**: sets out processes and procedures that must be followed when there is an actual or suspected information security incident e.g. loss or theft of personal data

4.2. Procedures

- **Data Protection Impact Assessment (DPIA) Procedure**

- **Subject rights procedures** e.g. procedures and forms relating to processing subject access requests

- **Data Processing Agreement template**

4.3. Guidance

- **Information disclosure guidelines**: provides advice about when personal data can be disclosed to third parties e.g. Police, local authorities, utility companies

- **Sending personal data by email guidance**: provides guidance to follow when sending personal data via email