Data Protection Policy

Overall purpose of policy

The purpose of this policy is to enable us to:

- ensure all employees are aware of the data protection process and how to manage any requests;
- comply with the requirements of the General Data Protection Regulation (GDPR) in respect of the data we hold about individuals;
- follow good practice;
- protect our customers, employees and other individuals; and
- protect us from the consequences of any breach of, or non-compliance with our responsibilities.

How the policy will be implemented

The Litigation Lawyer will lead on communication and through the actions outlined in this policy, will ensure:

- all employees are aware of this policy and their responsibilities under the GDPR and carry out their work in line with this policy;
- the policy is published on the Intranet;
- delivery of training to all relevant employees on data protection legislation; and
- best practice is followed and updates are provided by the Information Governance Group.

Performance measures

- Breaches of data protection legislation.
- Subject access requests completed within one month.
- Training relevant employees.

TARGETS

- No breaches of data protection resulting in action by the Information Commissioner's Office.
- All subject access requests completed within one month of receipt.
- All relevant employees undertake data protection training on an annual basis.

Date Approved By CMB: 22 May 2018
Date Due For Review: 31 May 2021
Responsible Officer: Litigation Lawyer

Data Protection Policy

1 Statement of Intent

1.1 This policy applies to personal information relating to a living individual who can be identified from that information or together with other information that we hold.

1.2 It applies to personal and special categories of data (see Appendix A for definitions), in any electronic and physical format. It sets out how we handle the personal information of our customers, employees, suppliers and other third parties.

1.3 The General Data Protection Regulation EU 2016/679 (GDPR) requires all organisations that handle personal information to comply with a number of important principles about privacy and disclosure.

1.4 The six principles limit the reasons for which personal data may be obtained and specify how it can be used. We adhere to the principles relating to processing of personal data set out in the GDPR, which require personal data to be:

- processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency);
- collected only for specified, explicit and legitimate purposes (Purpose Limitation);
- adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed (Data Minimisation);
- accurate and where necessary kept up to date (Accuracy);
- not kept in a form which permits identification of 'Data Subjects' for longer than is necessary for the purposes for which the data is processed (Storage Limitation); and
- 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 (Security, Integrity and Confidentiality).

1.5 We are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

1.6 We and our employees who process or use personal information will ensure the principles are followed at all times.

1.7 We recognise that the correct and lawful treatment of personal data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously. We are exposed to potential fines of up to approximately £17million or 4% of total worldwide annual turnover, whichever is higher.

2 Outline of Service

2.1 Responsibilities

Board

2.1.1 Our Board will make sure we comply with our legal obligations under data protection legislation.

Data Protection Officer

2.1.2 The Litigation Lawyer will act as Data Protection Officer. The Data Protection Officer will:

- inform and advise about the obligation to comply with the GDPR and other data protection laws;
- monitor compliance with the GDPR and other data protection laws, and with our data protection polices, including managing internal data protection activities, raising awareness of data protection issues, training employees and conducting internal audits;
- advise on, and monitor data protection impact assessments;
- cooperate with the supervisory authority; and
- be the first point of contact for supervisory authorities and for individuals whose data is processed.

Infrastructure Technology Manager

2.1.3 The Infrastructure Technology Manager will be responsible for security of the organisations networks and electronic devices.

Managers

2.1.4 Managers will support the implementation of data protection awareness, training and good practice within their teams.

2.1.5 Managers are responsible for implementing and monitoring compliance with this policy within their functional areas.

2.1.6 Managers must ensure the Data Protection Officer is consulted if they have any concerns about the following:

- consent and / or need to capture explicit consent;
- the retention period for personal data being processed;
- drafting Privacy Notices;
- security or other measures they need to implement to protect personal data;
- if there has been a personal data breach;
- if they need assistance with any rights invoked by a Data subject,
- a significant new, or change in , processing activity, which is likely to require a Data Protection Impact Assessment (DPIA); or
- any contracts or others areas in relation to sharing personal data with third parties.

Employees

2.1.7 Employees are required to read, understand, accept and work according to any policies and procedures that relate to the personal data they may handle in the course of their work.

2.1.8 All employees are responsible for:

- ensuring the information they give us in connection with their employment is accurate and up to date;
- informing us of any changes to their personal information, for example, changes of address; and
- immediately reporting any breaches of data protection to the Data Protection Officer and / or the Infrastructure Technology Manager.

Non-Compliance

2.1.9 Failure to comply with this policy may result in disciplinary action being taken.

2.2 Security

2.2.1 All employees will be responsible for the protection of data, and will take reasonable steps to ensure data security.

2.2.2 All data will be 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.

2.2.3 We will ensure regular reviews of our information security policies and procedures, to ensure we continually review the protection of data, both physical and electronic.

2.2.4 All employees are required to comply with the requirements of the Information Security Policy.

2.2.5 Access to information on the main computer system will be controlled according to job role.

2.2.6 The IT Service Desk and the Records Management Team will be notified of new starters, leavers and those changing post internally, to ensure effective access controls can be maintained.

2.2.7 All employees are responsible for making sure personal information is not disclosed, either orally, in writing, through web pages or by any other means, accidentally or otherwise, to any unauthorised third party.

2.2.8 For further information, please refer to the Information Governance Framework.

2.3 Data accuracy

2.3.1 All reasonable steps will be taken to ensure the accuracy of the personal data. We will update personal data from information obtained during regular reviews, for example, Homesearch Applications, and Care Link Update Forms.

2.3.2 Procedures will be in place so all relevant systems are updated when information is received about any individual changes.

2.3.3 A routine programme of data quality audits will be carried out to ensure data accuracy.

2.3.4 For further information, please refer to the Information Governance Framework.

2.4 Data Subject's rights and requests

2.4.1 'Data Subjects' have specific rights on how we handle their personal data, these include rights to:

- withdraw consent to processing at any time;
- receive certain information about the Data Controller's processing activities;
- request access to their personal data that we hold;
- prevent our use of their personal data for direct marketing purposes;
- ask us to erase personal data if it is no longer necessary to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;
- restrict processing in specific circumstances;
- challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
- request a copy of an agreement under which personal data is transferred outside of the EEA;
- object to decisions based solely on automated processing, including profiling (ADM);
- prevent processing that is likely to cause damage or distress to the Data Subject or anyone else;
- be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
- make a complaint to the supervisory authority; and
- in limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

2.4.2 All requests by a Data Subject will be responded to without undue delay and in any event within one month of receipt of the request (in the majority of circumstances).

2.5 Subject access

2.5.1 All subject access requests will be handled by the Data Protection Officer or delegated to a nominated member of the Records Management Team.

2.5.2 Subject access requests must be made in writing. All employees are required to pass on anything which might be a subject access request to the Data Protection Officer, and or Records Management Team within one working day.

2.5.3 Where an individual makes a subject access request their identity will be verified before any information is handed over.

2.5.4 We will respond to all subject access requests within the statutory timescale of one month.

2.5.5 For further information, please refer to the Subject Access Request Procedure.

2.6 Direct marketing

2.6.1 Individuals have the right to prevent their personal data being processed for direct marketing.

2.6.2 The right to object to direct marketing will be explicitly offered to Data Subjects in an intelligible manner so they can clearly distinguish it from other information.

2.6.3 A Data Subject's objection to direct marketing will be honoured promptly. Where a customer opts out at any time, their details will be suppressed as soon as possible. We will retain enough information to ensure that marketing preferences are respected in the future.

2.7 Retention of Data

2.7.1 Personal data will not be kept in a form, which permits identification of Data Subjects for longer than is necessary for the purposes for which it is processed. Different categories of data will be retained for different periods of time according to our Records Retention Schedule.

2.7.2 For further information, please refer to the Records Retention Schedule.

2.8 Confidentiality

2.8.1 Confidentiality applies to a much wider range of data than that covered by data protection legislation. All employees have a responsibility to maintain confidentiality of all data and information, to protect both people and the organisation.

2.8.2 Employees must not disclose confidential information to unauthorised people.

2.8.3 Employees are expected to withhold the information where there is any uncertainty about whether it should be disclosed, until they have checked with their line manager.

2.9 Lawfulness, fairness and transparency

2.9.1 Personal data will be processed lawfully, fairly and in a transparent manner in relation to a Data Subject. We will only collect, process and share personal data fairly, lawfully and for specified purposes. GDPR allows processing for specific purposes, some of which are set out below:

- the Data Subject has given his or her consent;
- the processing is necessary for the performance of a contract with the Data Subject;
- to meet our legal compliance obligations;
- to protect the Data Subject's vital interests; and
- to pursue our legitimate interests for purposes where they are not overridden because the processing prejudices the interests or fundamental rights and freedoms of Data Subjects.

2.9.2 To make sure personal data is processed fairly and transparently, we will ensure in obtaining data no person is deceived or misled as to the purposes for which their data is to be processed.

2.9.3 Where we intend to share personal information with other organisations or agencies we will have robust data sharing protocols, which meet the Information Commissioner's Office 'Data sharing code of practice'.

2.9.4 Our privacy statement will be published on our website and detail what we do with the information we gather and who we may share it with.

2.9.5 Where necessary, we will gain the consent (see definitions) of the Data Subject to share their personal data with other organisations.

2.9.6 In relation to processing of sensitive personal data, we will either obtain explicit consent, or rely on another lawful basis. Where we share personal data with other organisations we will ensure the sharing is fair and justified.

2.10 Privacy by Design and Data Protection Impact Assessment (DPIA)

2.10.1 We will implement 'Privacy by Design' measures when processing personal data, using appropriate technical and organisational measures (like pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

2.10.2 We will assess the Privacy by Design measures that can be implemented on all programs / systems / processes that process personal data, by taking into account the following:

- state of the art;
- cost of implementation;
- nature, scope, context and purposes of processing;
- risks or right for the freedoms of Data Subjects posed by the processing; and
- the Data Controller has conducted a DPIA in respect to high risk processing.

2.10.3 A DPIA will be conducted and the finding discussed with the DPO, when implementing major system or business change programs involving the processing of personal data. This includes:

- use of new or changing technologies (programs, systems or processes);
- automated processing including profiling and automated decision making;
- large scale processing of sensitive data; and
- large scale, systematic monitoring of a publicly accessible area.

2.10.4 We will comply with guidelines on DPIA and Privacy by Design. The Data Protection Impact Assessment Procedure provides further information on this process.

2.11 Data sharing

2.11.1 By 'data sharing' we mean the disclosure of data from us to a third party organisation.

2.11.2 There are two main types of data sharing (see Appendix B):

- systematic, routine data sharing where the same data sets are shared between the same organisations for an established purpose; and
- exceptional, one-off decisions to share data for any of a range of purposes.

2.11.3 Where we are the data controller (see definitions), in order to share personal data with another party that processes this data on our behalf (the data processor), the GDPR requires that we have a written contract in place. This imposes a number of mandatory terms on the data processor, as set out in the GDPR. In these situations, a separate data sharing agreement is not required.

2.11.4 We will have in place data sharing agreements and review them regularly, particularly where information is shared on a large scale, or on a regular basis. The Records Management Team will maintain a register of all data sharing agreements we have entered into.

2.11.5 Our Privacy Notice, accessible though our website, details what we do with the information we gather and who we may share it with. This approach is acceptable where the data sharing is something people are likely to expect or be aware of already, and to which people are unlikely to object.

2.12 Reporting a personal data breach

2.12.1 We are required to notify any personal data breach (see definitions) to the applicable regulator and, in certain instances, the Data Subject. We have a procedure in place to deal with any suspected personal data breach.

2.12.2 All employees who know or suspect a personal data breach has occurred, must report this immediately to the Records Management Team, the Infrastructure Technology Manager or Data Protection Officer, who are the designated point of contact for personal data breaches.

2.12.3 Employees must report any data breach or potential data breach without delay as we have a requirement to report a data breach to the Information Commissioner's Office within 72 hours.

2.12.4 We have a Personal Data Breach Plan, which provides further information on the reporting process.

3 Specific Needs

3.1 We will take into account the specific needs, which may arise, of older and vulnerable people, people with disabilities, and black, Asian and minority ethnic groups, in a manner that promotes equality and inclusiveness.

4 Consultation

4.1 No consultation has taken place as the policy is directed by changes to data protection legislation.

4.2 Future consultation will take place with the Information Governance Group on review or amendment to this policy.

5 Implementation

5.1 Our Board and Chief Executive are responsible for making sure that this policy is implemented.

5.2 Under the delegated authority within our Standing Orders it is the responsibility of all employees and those working on our behalf to ensure that their work is carried out in line with this policy and any related procedures.

5.3 We are committed to the highest standards of customer care and will apply this policy in accordance with the standards published in our Customer Charter Standards. If customers are dissatisfied with the service that they have received or with the application of this policy then they should refer to our Complaints and Compensation Policy.

6 Monitoring

6.1 Our Board will receive regular monitoring reports to evaluate the effectiveness of this policy in meeting customer expectations.

6.2 We will undertake surveys to monitor the satisfaction of our tenants with the service provided and will publish the results.

6.3 Where relevant information is available we will benchmark our performance against other organisations to ensure the highest standards of service delivery.

7 Review

7.1 We will undertake a review of this policy whenever there are any relevant changes to legislation, case law or good practice that would impact on this policy or in the light of any required service improvements identified through our Complaints and Compensation Policy.

7.2 We will constantly review service provision in line with best practice, and will undertake regular reviews to ensure continuous improvements and value for money in the delivery of our services.

7.3 Our Board will be responsible for ensuring that reviews of this policy are carried out and that the policy contributes to, and complements, our strategic objectives.

7.4 In carrying out any such review account will be taken of our commitment to diversity and inclusion.

For further information please refer to our Diversity and Inclusion Policy.

8 Risk

8.1 All risks that fall within the scope of this policy and its service areas have been identified and contained within our Risk Map and Management Plan with controls in place to make sure that the risks are managed effectively.

8.2 When reviews of this policy are undertaken, checks will be made against our Risk Map and Management Plan to ensure that the policy takes account of and addresses any relevant risks. Where the policy review identifies a material risk, not contained within the Risk Map and Management Plan the risk will be notified to the Business Excellence and Risk Manager and appropriate controls put in place.

For further information please refer to our Risk Map and Management Plan.

9 Legislation and Other Documents

9.1 Our Board will ensure that this policy complies with all relevant legislation and takes account of current best practice.

- General Data Protection Regulation 2016.
- Information Governance Framework.

Appendix A: Definitions

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.

Data Processor: the person or organisation that processes data on behalf of the Data Controller.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal Data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information, which is meant to be kept separately and secure.

Processing: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Special categories of personal data

Special category data is personal data, which the GDPR says, is more sensitive, and so needs more protection and which reveals an individual's:

- race;
- ethnic origin political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetics information;
- biometrics information (where to identify an individual);
- health information;
- sex life; or
- sexual orientation.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Appendix B: Data sharing checklists

Data sharing checklist – systematic data sharing

Scenario: You want to enter into an agreement to share personal data on an ongoing basis.

Is the sharing justified?

Key points to consider.

- What is the sharing meant to achieve?
- Have you assessed the potential benefits and risks to individuals and / or society of sharing or not sharing?
- Is the sharing proportionate to the issue you are addressing?
- Could the objective be achieved without sharing personal data?

Do you have the power to share?

Key points to consider.

- The type of organisation you work for.
- Any relevant functions or powers of your organisation.
- The nature of the information you have been asked to share. (For example, was it given in confidence?)
- Any legal obligation to share information (for example a statutory requirement or a court order).

If you decide to share

It is good practice to have a data sharing agreement in place. As well as considering the key points above, your data sharing agreement should cover the following issues.

- What information needs to be shared?
- The organisations that will be involved.
- What you need to tell people about the data sharing and how you will communicate that information.
- Measures to ensure adequate security is in place to protect the data.
- What arrangements need to be in place to provide individuals with access to their personal data if they request it?
- Agreed common retention periods for the data.
- Processes to ensure secure deletion takes place.

Data sharing checklist – one off requests

Scenario: You are asked to share personal data relating to an individual in 'one off' circumstances.

Is the sharing justified?

Key points to consider.

- Do you think you should share the information?
- Have you assessed the potential benefits and risks to individuals and / or society of sharing or not sharing?
- Do you have concerns that an individual is at risk of serious harm?
- Do you need to consider an exemption in the DPA to share?

Do you have the power to share?

Key points to consider.

- The type of organisation you work for.
- Any relevant functions or powers of your organisation.
- The nature of the information you have been asked to share. (For example, was it given in confidence?)
- Any legal obligation to share information? (For example, a statutory requirement or a court order.)

If you decide to share

Key points to consider.

- What information do you need to share?
  - Only share what is necessary.
  - Distinguish fact from opinion.
- How should the information be shared?
  - Information must be shared securely.
  - Ensure you are giving information to the right person.
- Consider whether it is appropriate to inform the individual that you have shared their information.

Record your decision

Record your data sharing decision and your reasoning – whether or not you shared the information.

If you share information you should record:

- what information was shared and for what purpose;
- who it was shared with;
- when it was shared;
- your justification for sharing; and
- whether the information was shared with or without consent.

(ICO's Data Sharing Code of Practice)