Data Protection Policy

1. BACKGROUND AND OBJECTIVES

1.1. Our commitment

1.2. We are committed to accountability and good governance in the processing of Personal Data and ensure:

- data is kept safe and secure
- data is handled legally, responsibly and ethically
- we are open and transparent about what data we are using and why
- we only collect what we need

1.3. Scope

1.4. This policy sets out our approach to compliance with data protection legislation and good practice across Westward Housing Group (Westward), including subsidiary entities of Sharewest Limited and (New) Horizon Homes (HH) Limited, and in our Help to Buy agency activities carried out jointly with HH and Sovereign Living Limited.

1.5. This policy covers compliance with General Data Protection Regulations (GDPR), Data Protection Act [legislation name to be confirmed], Information Commissioner's Office (ICO) guidance and other related legislation and regulations including:

- Payment Card Industry (PCI) Regulations - taking card payments over the phone
- Gender Recognition Act 2005 - criminal offence to disclose sensitive information about a transsexual person (whether they are transsexual or identify as transgender)
- Social Security (Information-sharing in relation to Welfare Services) Regulation 2012 and Welfare Reform Act 2012 - information sharing powers regarding benefit claims
- Privacy and Electronic Communications Regulations (PECR) 2011 – electronic marketing and website cookies
- Telephone Preference Service (TPS) and Corporate Telephone Preference Service (CTPS) - opt out for sales and marketing calls
- Crime and Disorder Act 1998 (Section 115) - sharing data
- Human Rights Act 1998 - binds public authorities to respect and protect individuals' human rights; including an individual's right to privacy (Article 8)
- Care Act 2014 and Children Act 2004 - safeguarding and data sharing

and our own definitions of confidentiality.

1.6. The policy applies to everyone who processes Westward data including staff, Non-Executive Directors, volunteers, involved residents and Data Processors (refer to relevant sections below).

1.7. Breaches of this policy and the law may impact the rights and freedoms of Data Subjects. The ICO has powers to sanction and/or fine organisations in breach of the law. We encourage reporting of breaches and near misses so we can mitigate the risks and learn from them.

1.8. We have appointed a Data Protection Officer (DPO) to lead on compliance and advice related to data protection. The DPO should be contacted regarding breaches, complaints, subject access requests or queries about rights.

1.9. This policy must be read alongside associated documents and related procedures noted at the end (also see Appendix A for data protection legislation definitions and terminology).

1.10. Data protection principles

1.11. We are responsible for, and are able to demonstrate, compliance with data protection principles that ensure Personal Data is:

1. **processed lawfully, fairly and in a transparent manner** using clear and plain language
2. **collected for specified, explicit and legitimate purposes** and not further processed in a manner that is incompatible with those purposes
3. **adequate, relevant and limited to what is necessary** in relation to the purposes for which they are processed
4. **accurate and kept up to date**; every reasonable step is taken to ensure Personal Data are accurate, having regard to the purposes for which they are processed, are erased or rectified without delay
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
6. processed in a manner that ensures appropriate **security**, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures

2. PROCESSING DATA

2.1. Personal Data

2.2. Personal Data includes any information relating to a living identified or identifiable individual ('Data Subject' or 'natural person'); this may include:

- name and contact details (including email, telephone numbers and current, previous and forwarding addresses)
- identification information (including age and gender)
- family details (including next of kin and marital status)
- financial information (including income, welfare benefit entitlements and bank account details)
- national identifiers (including National Insurance or social security number)
- education and employment details
- online identifiers (including IP address or cookies)
- device identifiers (for example identifiers for a smartphone)
- photographs, CCTV images, films and telephone recordings
- whistleblowing (confidential reporting) information

2.3. Personal Data includes information held manually (paper or written format) or electronically (emails, information on computer systems, social media, images, voice recordings, etc.).

2.4. Personal Data at Westward can be related to employees, volunteers, tenants, clients, service users, non-executive directors (board and committee members), members of the public, contractors, suppliers and more.

2.5. Personal Data can be provided by the Data Subject or a third party, such as a Doctor or the local authority.

2.6. Processing Personal Data

2.7. We need a lawful basis for processing Personal Data. The bases available are:

- **consent** of the Data Subject which should only be used when a genuine choice can be offered
- for the performance of a **contract** with the Data Subject or to take steps to enter into a contract
- for compliance with a **legal obligation** (including a court order)
- to protect the **vital interests** of a Data Subject or another person (i.e. life or death)
- for the performance of a task carried out in the **public interest** or in the exercise of official authority vested in the Data Controller
- in the **legitimate interests** pursued by the Data Controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the Data Subject

2.8. We consider each processing activity and record on our Information Asset Register (IAR) the lawful basis for each. Most of our processing activity relates to 'performance of a contract' (such as a tenancy agreement, support agreement or employment contract).

2.9. Sensitive Data

2.10. Sensitive Data or 'Special Categories of Personal Data' includes:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade-union membership
- physical or mental health status (past, current or future)
- disability
- sex life or sexual orientation
- genetic data
- biometric data (i.e. DNA, fingerprints and retina scans)

2.11. Processing Sensitive Data

2.12. The lawful bases available for processing Sensitive Data are summarised below for information (a more detailed list of bases is available on the intranet). For each processing activity we carry out, we will consider the appropriate legal basis.

- Explicit **consent** of the Data Subject
- Processing is necessary for carrying out **obligations** under employment, social security or social protection law, or a collective agreement
- Processing is necessary to protect the **vital interests** of a Data Subject or another individual (must be a matter of life or death)
- Processing carried out by a not-for-profit body with a **political, philosophical, religious or trade union aim** (unlikely to be appropriate for Westward processing activities)
- Processing relates to Personal Data **manifestly made public** by the Data Subject
- Processing is necessary for the establishment, exercise or defence **of legal claims** or where courts are acting in their judicial capacity
- Processing is necessary for reasons of substantial **public interest** (this is a detailed area and includes matters such as **equalities monitoring, fraud, unlawful acts, insurance,** etc)
- Processing is necessary for the purposes of **preventative or occupational medicine**, for assessing the working capacity of the employee, medical diagnosis, the provision of health or

social care or treatment or management of health or social care systems and services or a contract with a health professional
- Processing is necessary for reasons of public interest in the area of **public health**
- Processing is necessary for **archiving** purposes in the public interest, or scientific and historical research purposes or statistical purposes

2.13. In accordance with data protection legislation, we carry out appropriate equality and diversity monitoring in relation to Sensitive Data about racial/ethnic origin, religious/philosophical beliefs, health and sexual orientation. We do not use this monitoring data to make decisions about individuals, we use it to understand who we house and provide services to so we can consider if we are providing fair access.

2.14. Criminal offence data

2.15. Criminal convictions or offences data includes:
- the alleged commission of offences by the data subject, or
- proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing

2.16. It is dealt with in a similar way to Sensitive Data and we must have a lawful reason for processing (a detailed list of bases is available on the intranet).

2.17. Processing under Consent

2.18. Where we rely on consent for processing, it must be:
- freely given, specific, informed and unambiguous (in other words, they must choose to 'opt-in')
- separate from other terms and conditions
- simple to withdraw
- properly documented

2.19. Data subjects have these extra rights where we rely on consent to process their data:
- right to erasure (to be forgotten)
- right to object (in effect, withdraw consent)

2.20. We use our IAR to record the date consent was given, the mechanism (i.e. online clicks or positive agreement on the telephone) and explicitly re-request this consent every 2 years.

2.21. Consent guidelines and checklists are available on the intranet.

2.22. Processing under Legitimate Interest

2.23. Where we rely on Legitimate Interest we carefully consider the interests, fundamental rights and freedoms, and reasonable expectations of the Data Subject; if these are outweighed by our needs as a Data Controller we look for another lawful reason or do not carry out the processing. We document our decision on the IAR.

2.24. If our assessment identifies a significant privacy impact, we considered whether we also need to conduct a Data Privacy Impact Assessment (see below).

2.25. The processing of Personal Data for direct marketing purposes can be carried out under Legitimate Interest provided:
- our needs as do not override the Data Subject's needs (as noted above)
- marketing is limited to direct mail and telephone calls
- we comply with PECR, Telephone Preference Service (TPS) and Corporate TPS, as appropriate
- individuals are informed that data is being processed under Legitimate Interest (via Privacy Notice)
- we offer an 'opt-out'

2.26. We review direct marketing and use of legitimate interest when the IAR is reviewed or when we consider new processing activities.

2.27. Children's data

2.28. Children under the age of 18 years need particular protection when collecting and processing their Personal Data because they may be less aware of the risks, consequences and safeguards concerned.

2.29. Children have the same data rights as adults. We only allow parents to exercise these rights on behalf of a child when:
- the child authorises them to do so; or
- the child does not have sufficient understanding to exercise the rights themselves; or
- when it is evident that it is not in the best interests of the child to respond to the child instead of the parent.

2.30. Processing of children's data is noted within the Information Asset Register (IAR); this is reviewed regularly when the IAR is reviewed. We hold information on children in relation to their parent or guardian (i.e. as part of a tenancy agreement). We also have some support contracts with children (aged 16 and 17) and may hold photos of children for promotion and publicity purpose with consent. Currently we do not use children's data for direct marketing, automated decision-making or profiling.

2.31. Where appropriate, we design our processing with children in mind by:
- using Plain English (particularly in our Privacy Notice)
- having information accessible via the web and social media
- consulting children
- when relying on consent, making sure the child understands what they are consenting to and ensuring we do not exploit any imbalance in power in the relationship between us
- when relying on 'performance of a contract', considering the child's competence to understand what they are agreeing to
- when relying upon 'legitimate interests', taking responsibility for identifying the risks and consequences of the processing, and put age appropriate safeguards in place

2.32. Transgender data

2.33. Under the Gender Recognition Act 2005 it is a criminal offence to disclose sensitive information about a transsexual person (whether they are transsexual or identify as transgender), even accidently, without permission, if it was obtained in an official capacity; this applies to indirect as well as direct (word of mouth) disclosure and means the handling of relevant paper and computer records is considered with great care.

2.34. Access to records showing the change of name and any other details associated with the individual's transsexual status (i.e. assessments, support notes, etc.) is restricted to specified staff who require

the information to do their work. Once a person has obtained a Gender Recognition Certificate, there must be no disclosure of this information.

2.35. We have a procedure for updating our systems when an individual's gender status changes (available on intranet).

2.36. Recording processing activities

2.37. We have carried out an information audit across the whole of Westward to record all Personal Data held and processed; this is documented in the Information Asset Register (IAR) which is reviewed annually and updated whenever we carry out a new processing activity.

2.38. We maintain a Record Of Processing Activities (ROPA) using information from our IAR and other sources:

ROPA	Westward compliance evidence
• our organisation name and details, including DPO	• Privacy Notice • DPO info within this policy
• the name and contact details of any joint controllers	• IAR • Privacy Notice
• purposes of the processing	• IAR • Privacy Notice
• description of the categories/classes of individuals (i.e. staff, Non-Executive Directors, customers, etc.)	• IAR • Privacy Notice
• description of the categories of Personal and Sensitive Personal Data we process (i.e. contact details, health info, etc.)	• IAR • Privacy Notice
• recipients of Personal Data (i.e. contractors, partners, etc.)	• IAR • Privacy Notice • Data Sharing Register • Data Processor Register
• transfers outside of UK	• IAR (none currently)
• retention schedules	• Retention Schedule (see below)
• general description of technical and organisational security measures (i.e. encryption, training, access controls, etc.)	• Below and within IS User Policy

3. DATA CONTROLLERS AND PROCESSORS

3.1. Westward as a Data Controller and a Data Processor

3.2. Westward is a Data Controller as we collect and process Personal Data, and determine when and how it is to be processed.

3.3. Westward is occasionally a Data Processor (i.e. receiving data from other organisations in order to carry out gas servicing or repairs, and as the Help to Buy joint agent with Homes England); we must comply with data protection legislation and data processing agreements.

3.4. Using Data Processors

3.5. If we (as the Data Controller) provide information to a third party (Data Processor) in order for them to perform a service for us (i.e. a mailing house, payroll provider, maintenance contractor, etc.) we must ensure the contract complies with data protection legislation.

3.6. There are specific legal obligations on the Data Processor (i.e. maintenance of records of Personal Data and processing activities) and liability where the Data Processor is responsible for a breach (see breach section below).

3.7. Any sub-contractors to the Data Processor must be notified to us as the Data Controller; they should be bound by same terms as main Data Processor.

3.8. We use a template Data Processor contract (including the requirements of Article 28) and hold a Register of Data Processors.

4. RIGHTS

4.1. Summary of rights

4.2. Data protection legislation provides the following rights for Data Subjects:

Individual rights	**Details of rights**	**Westward compliance evidence**
The right to be **informed** about Data Processing	• Obligation to 'fair processing information' • Transparency in use of Personal Data	• Privacy Notice
The right of **access** to Personal Data	• Subject Access Request (SAR) • Access to Privacy Notice information	• See policy section below • Procedure • Privacy Notice • Website portal
The right to **restrict** processing	• 'Block' or suppress processing of Personal Data • Storage of just enough information but no processing	• See policy section below
The right to **rectification**	• Inaccurate or incomplete Personal Data is rectified 'without undue delay'	• See policy section below • Website portal
The right to data **portability**	• Obtain and reuse own Personal Data • Applies where consent given or Data is used in the performance of a contract (no other grounds)	• See policy section below
Rights in relation to **automated decision making** and **profiling**	Falls into either: 1) Necessary for entering into or performance of a contract OR has Data Subject's consent 2) Direct marketing purposes where explicit consent not required but Data Subject can object	• Monitored via IAR
The following rights only apply where processing relies on consent:		
The right to **erasure**/be forgotten	• Right to have data erased 'without undue delay' where no compelling reason to process Personal Data or consent withdrawn	• See policy section below

The right to **object**	• Where Personal Data processed for direct marketing, Legitimate Interest or Public Interest • Unless Data Controller demonstrates compelling legitimate grounds for processing which overrides interests, rights and freedoms of Data Subject	• See policy section below

4.3. Right to be informed (Privacy Notice)

4.4. Information we provide about processing of Personal Data must be:
- concise, transparent, intelligible and easily accessible
- written in clear and plain language
- free of charge

4.5. A Privacy Notice explains our compliance with data protection legislation and our commitment to good data protection practices. Westward has a layered approach to Privacy Notices so that different customer groups can understand how their data is processed (i.e. tenants/support clients, employees, Non-Executive Directors, etc.). The full Privacy Notice is available on our websites, we also reference and summarise the Privacy Notice on forms we use to collect new data.

4.6. We review our Privacy Notice annually, or whenever we changes processing activities, and keep copies of previous versions in the event of queries.

4.7. Right of access (Subject Access Request or SAR)

4.8. Individuals have the right to obtain:
- access to their personal data (so they are aware of and can verify the lawfulness of the processing)
- confirmation that their data is being processed
- the purpose of holding it (the legal basis)
- the categories of Personal Data that have been collection (contact details, etc.)
- the sources of Personal Data
- who it is shared with (third parties)
- how long it will be held (retention)
- information about their rights and the right to complain to ICO
- other supplementary information (this largely corresponds to the information provided in a Privacy Notice)

4.9. A SAR can be made by an individual or a third party acting with their authority; verification of identity is required.

4.10. Information must be provided without delay and at the latest within one calendar month of receipt. We are able to extend the period by a further two months where requests are complex or numerous. If this is the case, we inform the individual within one month of the receipt of the request and explain why the extension is necessary.

4.11. Where we process a 'large quantity of information' concerning the Data Subject, we can request they specify the information or processing activities to which the request relates. There is no exemption for requests that relate to large amounts of data, however we may be able to refuse if we can demonstrate that the request is manifestly unfounded or excessive.

4.12. There is no charge for the first SAR. A 'reasonable fee' (based on administrative costs) can be charged for further copies of the same information.

4.13. Where requests are manifestly unfounded or excessive, in particular because they are repetitive, we can either:
- charge a reasonable fee taking into account the administrative costs of providing the information
- refuse to respond and explain why to the individual, informing them of their right to complain to the ICO and to a judicial remedy without undue delay and at the latest within one month

4.14. If the request is made electronically, we can provide the SAR information in a commonly used electronic format. We may also direct resident customers to our secure self-service portal to access their data.

4.15. The SAR is usually dealt with by the Housing Officer or Support Service manager, with support and advice from the DPO. The DPO keeps a log of SARs and provides advice and checks.

4.16. SAR procedures are available on the intranet.

4.17. Right to portability

4.18. This new right is designed to make it easier for Data Subjects to switch between service providers.

4.19. Data Subjects have the right to receive a copy of their own Personal Data in a 'structured, commonly used, machine-readable and interoperable format' and the right to transmit it to another Data Controller, where 'technically feasible'. We cannot charge a fee.

4.20. The right to portability applies only when processing is based on consent or performance of a contract; it does not give rights in respect of:
- manual (paper) Personal Data
- Personal Data that has not been provided directly by the Data Subject to the Data Controller (such as an Occupational Therapist report generated by Westward)
- Personal Data processed for the 'performance of the task carried out in the public interest or in the exercise of official authority vested in the Controller' (such as where Westward delivers a homelessness support contract for the local authority)

4.21. We will seek appropriate verification before carrying out action in response to a request.

4.22. Requests must be dealt with without undue delay and within at least one calendar month; this may be extended by 2 months where the request is "complex".

4.23. We will consider the need to keep the data after portability has occurred; this will be reviewed using our retention procedures.

4.24. Portability procedures are available on the intranet [to be developed].

4.25. Right to rectification (correction)

4.26. Individuals are entitled to have Personal Data rectified if it is inaccurate or incomplete.

4.27. We will seek appropriate verification before carrying out action in response to a request; this is to ensure that we comply with other legislation and the related contracts (such as tenancy agreement).

4.28. We have one calendar month in which to respond; this can be extended by two months where the request is 'complex'.

4.29. Where we decide not to take action in response to a request for rectification, we must explain why and inform the individual of their right to complain to the ICO and to a judicial remedy.

4.30. Where we have disclosed the Personal Data in question to third parties, we must inform them of the rectification, where possible. We must also inform the individuals about the third parties to whom the data has been disclosed where appropriate.

4.31. Rectification procedures are available on the intranet [to be developed].

4.32. Right to erasure (to be forgotten)

4.33. Where we are processing data under consent, individuals have a right to have Personal Data erased and prevent processing in these circumstances:

- the Personal Data is no longer necessary in relation to the purpose for which it was originally collected
- the individual withdraws consent
- the individual objects to the processing and there is no overriding Legitimate Interest for continuing the processing
- the Personal Data was unlawfully processed (a data protection breach)
- the Personal Data has to be erased in order to comply with a legal obligation

4.34. We can refuse to comply with a request where Personal Data is processed for the following reasons:

- to exercise the right of freedom of expression and information (i.e. journalistic purposes)
- to comply with a legal obligation (i.e. the Data Subject has an outstanding debt)
- for public health purposes in the public interest (i.e. health threats)
- historical, statistical and scientific research purposes

We may retain a bare minimum amount of Personal Data in order for supress the data from being used again (an Erasure Register [to be developed]) for the reasons above and below:

- archiving purposes in the public interest
- for the performance of a public interest task or exercise of official authority
- the exercise or defence of legal claims

4.35. We will seek appropriate verification before carrying out action in response to a request.

4.36. Where we have disclosed Personal Data to third parties, we must inform them about the erasure, unless it is impossible or involves disproportionate effort to do so. We must also inform Data Processors and, if they hold data on that individual, they must comply with the request.

4.37. Erasure procedures are available on the intranet.

4.38. Right to restrict processing

4.39. Restricted processing is when we are permitted to store but not process Personal Data unless for the purpose of legal claims, protecting the rights of another person or for important Public Interest. We can retain just enough information to ensure the restriction is respected in future and would hold this on a Restriction Register [to be created].

4.40. We are required to restrict the processing of Personal Data in the following circumstances:

- an individual contests the accuracy of the Personal Data, we should restrict the processing until we have verified its accuracy
- an individual has objected to processing and we are considering whether our Legitimate Interests override those of the individual

- when processing is unlawful (a data protection breach) and the individual opposes erasure and requests restriction instead
- we no longer need the Personal Data but the individual requires the data to establish, exercise or defend a legal claim

4.41. Where we have disclosed the Personal Data to third parties, we must inform them about the restriction on the processing, unless it is impossible or involves disproportionate effort to do so.

4.42. We inform individuals when we decide to lift a restriction on processing.

4.43. Restriction procedures are available on the intranet [to be developed].

4.44. Right to object

4.45. Where we process data under consent, individuals have the right to object to:
- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling)
- direct marketing (including profiling)
- processing for purposes of scientific/historical research and statistics

4.46. Where we process data for the performance of a legal task or Legitimate Interest, individuals can object and we must stop processing the personal data unless:
- we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or
- the processing is for the establishment, exercise or defence of legal claims.

4.47. Individuals must have "grounds relating to his or her particular situation" in order to exercise their right to object to processing for research purposes.

4.48. Where we are conducting research where the processing of Personal Data is necessary for the performance of a public interest task, we are not required to comply with an objection to the processing.

4.49. We inform individuals of their right to object at the point of first communication and in our Privacy Notice.

4.50. Where we process activities online, we provide a way for individuals to object online.

4.51. We will seek appropriate verification before carrying out action in response to a request.

4.52. Objection procedures are available on the intranet [to be developed].

4.53. Automated decision-making

4.54. Individuals may request that when a decision has been made about them, based solely on automated processing (i.e. an online credit application), that the processing is reviewed by a person rather than a machine.

4.55. As part of the online Help to Buy application, there is automated decision-making as applicants must meet certain criteria in order to be eligible for the scheme. Customers can contact Help to Buy if they wish to query this decision. Westward does not use any other automated decision-making; this is reviewed regularly when the IAR is reviewed.

4.56. Profiling

4.57. Profiling is any form of automated processing intended to evaluate certain personal aspects of an individual, in particular to analyse or predict:

- performance at work
- economic situation
- health
- personal preferences
- reliability
- behaviour
- location
- movements

4.58. There are two types of profiling:

- Profiling with legal or similarly significant effects, i.e. profiling from which 'decision are based that produce legal effects concerning him or her or similarly significantly affects him or her'.
- Other profiling without such effects (including most profiling for direct marketing purposes, for which explicit consent is not required but a Data Subject has the right to be informed at the first point of contact, and the right to object and their Personal Data no longer processed for that purpose).

4.59. Profiling with legal or similarly significant effects is only allowed if one of these conditions is met. The decision (arising out of the profiling):

- is necessary for entering into, or performance of, a contract between the data subject and a data controller; or
- is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
- is based on the data subject's explicit consent (if they opt-out, we must explain the consequences).

4.60. Westward does not currently undertake the kind of profiling that has a legal or similar significant effect; this is reviewed regularly when the IAR is reviewed.

5. SHARING DATA

5.1. Information sharing can be a difficult area and it is important to take time to consider the rights of the individual(s) concerned and the legal and regulatory responsibilities of the third parties and Westward.

5.2. Data sharing can take place:

- as a requirement of law or regulation (i.e. payroll data shared with HMRC)
- under a Data Sharing Agreement (DSA) set up with the third party or an Exchange Protocol set up with multiple parties
- ad hoc or one off requests (where these become more regular requests, a DSA should be set up)
- with permission of the individual(s) concerned (i.e. permission from a customer for their MP to raise their issue with us)

5.3. All sharing request are considered on a case by case basis using the guidance available on the intranet and these principles:

- verify the requester (call them back or verify their email)
- check for existing DSA or Exchange Protocol and follow it
- understand and justify the purpose(s) of sharing (i.e. legal requirement)
- record your decision to share (or not to share) on Open Housing, Case Management or another appropriate system
- only share what is necessary for the purpose
- provide the information securely (i.e. encrypted email or password protected document)
- the duty to share information can be as important as the duty to safeguard the individual and their confidentiality - consider the safety and well-being of the individual and others who may be affected by their actions
- consider whether it is appropriate/safe to inform the individual that you have shared their information
- if in doubt consult your manager and/or the DPO

5.4. We share essential information with utilities as we have a legitimate interest in making sure that utility charges are directed to those responsible; this is included in the Privacy Notice.

5.5. Data Sharing Agreements (DSA) and Exchange Protocols (EP)

5.6. There are DSAs in place (available on the intranet) and these should be checked before sharing.

5.7. Some services operate EPs with other agencies (available on the intranet) and the Nominated Officer should be consulted. These protocols include:

- MAPPA (Multi-Agency Public Protection Arrangements) is a process for assessing and managing risks to the community posed by several categories of high risk offenders and is led by the Police, Probation and Prison services.
- MARAC (Multi-Agency Risk Assessment Conferencing) is a process for identifying victims of domestic abuse most at risk from violence; the risk information is shared with relevant agencies to promote the safety of abuse victims and their children.
- Crime and Disorder Protocol
- [currently gathering info on sharing protocols – to be completed by June]

5.8. Permission (including relatives, MPs and Councillors)

5.9. Where a relative, MP, Councillor or other third party acts with the authority of an individual we can respond directly to them in relation to the matter raised. We must not release any information about unrelated third parties (i.e. information about a neighbour) without permission as this would be a breach.

5.10. Legislation - safeguarding

5.11. Westward has a duty to co-operate with local authorities implementing their statutory duties around adult and children safeguarding.

5.12. All Westward staff are trained in safeguarding. There are sharing flowcharts in the safeguarding adults and children policies and guidance is available on the intranet.

5.13. Our safeguard lead officer is the Head of Support Services. They are responsible for ensuring that information shared about individuals alleged to have caused harm is in accordance with human rights, data protection and confidentiality requirements, and that appropriate sharing protocols are in place.

5.14. Other legislation and regulation

5.15. Other legislation requires us to share data, here are some of the more common one:

5.16. We are authorised to share information relating to welfare benefits (such as Universal Credit) under the Social Security (Information-sharing in relation to Welfare Services) Regulation 2012 and Welfare Reform Act 2012.

5.17. Any person may disclose information to a relevant authority under Section 115 of the Crime and Disorder Act 1998, 'where disclosure is necessary or expedient for the purposes of the Act (reduction and prevention of crime and disorder)'. Relevant authorities include police, local authority, social housing providers, probation service, NHS, fire services, local probation boards.

5.18. Individuals have a right to respect for their private life under Article 8 of the European Convention on Human Rights. This is not an absolute right and can be overridden if necessary and in accordance with the law. This means that any interference must be justified and for a particular purpose: 'for example, protection of a person's health, prevention of crime, protection of the rights and freedoms of others'.

6. VOICE, IMAGE AND ONLINE DATA

6.1. Voice recordings

6.2. We record telephone calls for training and monitoring purposes. We inform callers via an automated message at the beginning of each incoming telephone call and via our Privacy Notice.

6.3. Recordings of calls may be used by us:

- for staff training to develop confidence and potential of staff
- to check and measure whether we meet standards agreed with residents
- for use in appraisals with staff to develop customer service
- as evidence where there are disputes
- as evidence in investigations concerning either our customers or staff
- to resolve complaints regarding abusive telephone calls involving either our customers or staff

6.4. Access to call recordings is through sampling, except for training purposes or when abusive or threatening behaviour has occurred or a complaint has been made and requires investigation. Access to these types of calls requires authorisation by the Chief Executive or Executive Director of Organisation and Workforce.

6.5. Payment cards recordings

6.6. The Payment Card Industry (PCI) Regulations require us to ensure that credit and debit card payments are dealt with in a specific way. We have set up our telephones to stop voice recordings when a card payment is made; the operation of this is monitored by random sampling carried out monthly by our IT team.

6.7. Staff are trained in the appropriate processing of card payments.

6.8. CCTV

6.9. We use CCTV at our offices and in some residential schemes and projects to prevent crime and ensure safety of occupants and visitors.

6.10. CCTV is classed as a high risk activity when monitoring large scale public areas and Data Subjects may include vulnerable people; this means that we will carry out a DPIA on our CCTV activities and review them annually or sooner when there are changes proposed using a checklist.

6.11. We hold a register of CCTV locations and ensure that signage is provided to inform Data Subjects.

6.12. Photos, films and videos

6.13. We use staff photos for ID badges and staff directories (such as within our intranet, phone system and email system). We use staff photos and films for promotional reasons (i.e. leaflets, intranet, websites and social media) under Legitimate Interest; staff can opt out if providing a specific reason.

6.14. We use Non-Executive Director photos under Legitimate Interest for identification, reference and promotion of the organisation online and in print.

6.15. Where we photograph or film individual or small groups of customers for promotional material we gain consent using our Photo Consent Form. If we film or take photos at an event, we will put up notices (where practical) to inform attendees of their right to opt out and how to do so.

6.16. Websites, live chat and social media

6.17. We operate these websites:

- Westward Housing Group: www.westwardhousing.org.uk
- Horizon Homes: http://www.horizonhomes.co.uk/
- Help to Buy (jointly with Sovereign Living): https://www.helptobuysw.org.uk/
- Grow horticulture social enterprise: http://www.grow-jigsaw.org.uk/

6.18. Cookies are small text files that are placed on your computer by websites you visit; they are widely used in order to make websites work faster and more efficiently for your benefit, as well as to provide information to the site owners so they can improve the site for customer preference. Visitors to Westward websites are provided with sufficient information to make a decision about whether they consent to cookies.

6.19. Live chat is not currently used but may be introduced. Transcripts would be added to appropriate systems to ensure they are accessible.

6.20. We have a presence on social media via Facebook, Twitter, Instagram, Linked In and YouTube. We remind customers that they can access their own contributions to social media when we deal with a Subject Access Request.

7. DATA RETENTION AND CLEANSING

7.1. We only store information for as long as is reasonably necessary for us to fulfil the purposes set out in the Privacy Notice; usually a maximum of six years after we cease to have a relationship with an individual or if we are in dispute, until legal proceedings have ended, whichever is longer.

7.2. We have adopted the National Housing Federation (NHF) Data Retention Schedule (available on the intranet) with the addition of:

- support customer personal files - kept for two years after support has ended
- support applications for accommodation - stored separately and kept for six years
- all unsuccessful support service referrals - kept for one year
- telephone calls are kept for up to 12 months and calls that are deemed abusive or threatening are kept until any investigation action is completed
- CCTV images are retained for up to a month [consulting on this] or until any investigative action is completed
- Fraud/bribery/money laundering data kept for a maximum of 6 years until any investigative action is completed
- Non-Executive Director unsuccessful applications are treated the same as unsuccessful employment applications

Where the NHF Schedule is silent, we will make a judgement and record our decision.

7.3. We annually review the data we hold to ensure it is not excessive and securely dispose of it in accordance with the Data Retention Schedule. Paper documents are shredded and electronic documents are deleted (where there is functionality we run a verification report before deletion).

7.4. Where data is retained but no longer needs to be in a personally identifiable format (such as for statistical purposes or monitoring equality and diversity), we will consider the use of anonymization (removing personal data) or pseudonymisation (replacing personal data with, for example, 'hash out' NI numbers).

7.5. ICO acknowledge that technical reasons may prevent the deletion/anonymisation of all Personal Data and accept that data may instead be put 'beyond use' (such as backup tapes stored securely off site) provided we follow these safeguards and guidelines:

- we cannot/will not try to use the data to inform decisions on an individual or use the data in a way that affects the individual
- we do not give other organisations access to the personal data
- we have appropriate organisational and technical security applied to the data
- we commit to permanent deletion if/when possible
- we erase what is 'reasonable' e.g. data may be kept if there is still a legal ground for processing, or if the data is still necessary in relation to the purposes for which it was collected or processed.

8. BREACHES

8.1. A breach occurs when action or inaction leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data.

8.2. Breaches are broadly in 3 categories:

- **Confidentiality breach** - unauthorised or accidental disclosure of, or access to, personal data, for example:
  - sending an email/letter to the wrong address
  - overheard conversations
  - inadvertently disclosing Personal Data over the telephone or in person
  - emailing Sensitive Personal Data without encryption
  - copying information to an employee's personal email or home computer system
  - unauthorised access to filing systems or software holding personal (such as CCTV, data systems, offices, notes, etc.) including hacking
  - theft or loss of documents, phones, tablets or other electronic devices

- **Integrity breach** - unauthorised or accidental alteration of personal data, for example:
  - changing data without verification
- **Availability breach** - accidental or unauthorised loss of access to, or destruction of, personal data, for example:
  - insecure disposal of paperwork
  - cyber-attack
  - loss of access to systems for a period of time

8.3. Everyone is responsible for reporting breaches, potential breaches and near miss data incidents to the DPO who will oversee the process and keep a Data Breach Register.

8.4. Where a breach occurs within a Data Processor's remit, the Data Processor must also report the breach to us as the Data Controller.

8.5. We have robust Data Breach Procedure that include:
- Identifying and reporting
- Initial mitigation and containment
- Notification of ICO and/or individual(s)
- Action plan and lessons learnt

8.6. We will consider the details of each breach in order to understand the likelihood and severity of the resulting risk to individual(s) rights and freedoms (i.e. risk of identity theft, financial loss, loss of confidentiality, risk to safety or any other significant economic or social disadvantage). This will determine whether we need to report it to the ICO and/or the individual(s) concerned.

8.7. Notifying the ICO

8.8. There is a duty to report a breach to ICO within 72 hours of becoming aware of the breach (where feasible) where the breach is likely to result in a risk 'to the rights and freedoms' of individuals. Where this information is not all available at the time of reporting, information can be provided to ICO in phases.

8.9. Notifying individuals

8.10. Where a breach is likely to result in a 'high risk' to an individual's rights and freedoms (which is a higher threshold than for notifying the ICO) we will communicate with the individual(s), without undue delay and in plain English.

8.11. Breach consequences and lessons learnt

8.12. The ICO has the power to fine organisations breaching data protection legislation and individuals have a right to bring legal proceedings and claim compensation.

8.13. Depending on the nature of the breach and any action/inaction by persons or contractors acting on behalf of Westward, will be managed via the appropriate process (i.e. staff disciplinary or capability policies, Non-Executive Director conduct policy, contractor agreements, etc.).

8.14. The Data Breach Register and 'near miss' log are reported to Executive Team twice a year and Audit Committee annually, together with remedial action and lessons learnt. This learning will be shared with staff via staff briefings and, where appropriate, refresher training provided.

9. ACCOUNTABILITY

9.1. 'Privacy by Design'

9.2. 'Privacy by Design' is a legal requirement that to consider "appropriate technical and organisational measures" to protect the rights of Data Subjects and ensure data protection is built into projects and services.

9.3. Data Privacy Impact Assessments (DPIA)

9.4. We carry out a DPIA when using new technologies or assessing whether processing is likely to result in a risk to the rights and freedoms of individuals. The DPIA will help us understand and mitigate risks before processing begins.

9.5. Our DPIA guidance and template is available on the intranet and we keep a DPIA Register.

9.6. Our DPIAs are re-assessed every 3 years or sooner if changes in processing, good practice, etc.

9.7. Security

9.8. Our IS Usage Policy covers information systems access and security arrangements. The policy ensure appropriate technical and organisational measures are taken against unauthorised or unlawful processing or access and against accidental loss, destruction or damage. This includes restricting access to offices (via fobs, sign in sheets, etc.) and information systems (via passwords, read/write/view access, etc.).

9.9. We verify callers before discussing information with them.

9.10. Disaster recovery and business continuity

9.11. Data protection legislation requires us to ensure Personal Data is available. In the event of a disaster (for example a fire at the office) we will use our Business Continuity Plan to recover services and data. Loss of or lack of access to Personal Data must be reported to the DPO as this is a data breach.

9.12. Risks

9.13. We recognise the main risks are in the sharing of data and potential breaches by staff. These are mitigated by staff training and awareness raising (see below), sharing agreements and protocols, and monitoring of trends and lessons learnt.

9.14. Training

9.15. Data protection training is provided to all staff and is split into:

- Subject Access Request (SAR) training for those responsible for provide SARs
- overview of data protection legislation and how to ensure compliance for managers
- data protection legislation and how it impacts every working day

9.16. Refresher training for staff is provided every 2 years. New staff receive training as part of their induction.

10. CONFIDENTIAL AND INTERNAL INFORMATION

(This section is not a direct requirement of data protection legislation as it relates to more than just Personal Data)

10.1. Internal information should only be disclosed as part of legitimate business arrangements (i.e. as part of a tender submission or discussions with business partners).

10.2. Confidential information has restricted access as it could relate to sensitive personnel or organisation issues.

10.3. Commercially confidential information (i.e. Horizon Homes board papers) must be kept within Westward except with prior approval from a member of Executive Team or a board chair.

10.4. Westward is not classed as a public body under the Freedom of Information Act 2001 or Environmental Information Regulations 2004; this legislation is not applicable to us.

10.5. If in any doubt as to the nature of confidential and internal information employees should refer to their contract of employment or consult their manager, non-executive directors should consult their Chair and volunteers consult their manager.

10.6. Mail received by Westward which is clearly marked "confidential/private/addressee only" will be passed unopened to the person concerned unless otherwise authorised (i.e. PAs and correspondence addressed to non-executive directors).

11. RESPONSIBILITIES

11.1. Data Protection Officer (DPO)

11.2. The DPO is the Corporate Support Manager. The DPO is not personally responsible for compliance as this is the responsibility of the Data Controller (Westward Housing Group) and any Data Processors.

11.3. In summary the DPO's duties are to:

- inform and advise the organisation and employees about their obligations to comply with data protection legislation
- monitor compliance with data protection legislation, including managing internal data protection activities, train staff and conduct internal audits
- provide advice on data breaches, DPIAs and SARs
- be the first point of contact for ICO and Data Subjects
- report to the IT Governance Group, Board and Executive Team

11.4. The Data Controller must support the DPO and allow them to carry out their legal duties as set out in data protection legislation.

11.5. Any concerns about data processing and confidentiality must be reported promptly to the DPO or via the Whistleblowing (Confidential Reporting) Policy.

11.6. The DPO can be contacted via dataprotection@westwardhousing.org.uk

11.7. The DPO is responsible for the review and implementation of this policy.

11.8. Staff, Volunteers and Non-Executive Directors

11.9. All staff and volunteers must comply with all policies as part of their contract. They must also sign up to the IS Usage Policy and are bound by the statements on confidentiality within their contract and the Staff Handbook.

11.10. Non-executive directors sign up to the Board Member Agreement and receive confidentiality and data protection information at induction.

11.11. Involved residents sign up to a Code of Conduct when they get involved and are introduced to confidentiality and data protection at induction.

11.12. Managers and data owners (as set out in the IAR) are responsible for ensuring systems and processes enable and encourage data users to maintain fair and lawful data processing and confidentiality practices as described in this policy.

11.13. Westward board is responsible for ensuring compliance with data protection laws.

12. MONITORING, CONSULTATION AND REVIEW

12.1. Monitoring includes:

- breach and near miss reports to Executive Team twice a year and Audit Committee annually
- reporting any significant breach to Executive Team immediately
- oversight by the IT Governance group in relation to projects that may impact on compliance with data protection legislation or mitigate related risks

12.2. Staff Forum, Customer Senate and Customer Communications Group are consulted on updates to Privacy Notices and customer facing documents related to this policy.

12.3. Managers and key staff are consulted on updates to guidance and procedures related to this policy.

12.4. The practical operation of this policy is monitored to ensure that it is effective and compliant. The policy will be reviewed within a year of the new GDPR introduction. It will then be reviewed every 2 years, or sooner if good practice, regulation or legislation changes.

13. EQUALITY AND DIVERSITY

13.1. Westward aims to implement policies and procedures that support and meet the diverse needs of its stakeholders, ensuring that no one is placed at a disadvantage over others and to minimise, and if feasible, remove any disproportionate impact on the grounds of the nine protected characteristics under the Equality Act 2010. This policy and procedure operates without detriment to any employee on grounds of gender, race, ethnic origin, nationality, age, disability, religion or belief, sexual orientation or work pattern.

13.2. When applying this policy we will act sensitively towards the diverse needs of individuals and to reduce discrimination and harassment by:

- ensuring Personal Data and Sensitive Personal Data is handled in accordance with data protection legislation and this policy
- ensuring consent and opt outs can be managed in other languages or formats such as braille or BSL
- restricting the collection and processing of transsexual or gender reassignment data
- collecting and processing protected characteristic information in a sensitive and useful manner

14. ASSOCIATED DOCUMENTS

14.1. There are many associated documents linked to this policy; here are the key ones:

- National Housing Federation (NHF) data retention schedule
- IS Usage Policy
- Business Continuity Plan
- Disciplinary Policy
- Tenant handbook including leaflet 'how we use, safeguard and share your personal information'
- Complaints Policy
- Compensation Policy
- Safeguarding adults and children policies
- Whistleblowing (confidential reporting) Policy
- Staff handbook
- Contract of Employment
- Board Member Agreement for Services
- Privacy Notice
- Subject Access Request Guidance
- Data Breach Procedure
- Data Breach Register
- Data Processing Register
- Data processing contract addendum
- CCTV checklist
- Data Sharing Guidance
- Data Sharing Register
- Transgender data – systems update procedure
- Other rights guidance (erasure, portability, etc)

15. APPROVAL DATES

Version/Date	**Consultation & Approval Process**				**Review**
	Staff/Stakeholders	***Committee/ Board***	***ET***	***Staff Forum***	
GDPR update May18	Leadership Academy and Customer Comms Group – various documents	Update on GDPR Jun18	21May18	10May	May 2019

Appendix A – Glossary of data protection legislation terms

Consent: Any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by a statement or a clear affirmative action which signifies agreement to the processing of Personal Data.
Data breach: An occurrence which results in the security or accessibility of Personal Data held by the Data Controller or Data Processor being compromised.
Data Controller: The organisation that collects personal data and decides how it will be used.
Data Processor: The organisation that processes personal data on behalf of the data controller.
Data Protection Impact Assessment (DPIA): A method of identifying possible risks to privacy from a specific processing activity.
Data Protection Officer (DPO): An individual or legal entity appointed to inform and advise the data controller or the data processor and the employees who carry out processing of their obligations under data protection legislation. Identifier: Information from which an individual could be identified.
Data Processor Agreement (DPA): formal contract clause or addendum that sets out the responsibilities of the Data Processor
Data Sharing Agreement (DSA): formal agreement between Data Controllers that sets out what and how data can be shared.
Information Asset Register (IAR): records all Personal Data held and processed by us
ICO: Information Commissioner's Office, the data protection regulator
Joint Controller: The organisations that jointly collect personal data and decide how it will be used.
Legitimate interests (LI): Processing conducted in the interests of the data controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the individual.
Personal Data: Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Privacy Notice: Formal notice to be provided at the point of data collection that informs the Data Subject how we process information.
Processing: Any operation performed on personal data. This includes recording, structuring, storing and any form of analysis using personal data.
Profiling: Any form of automated processing of personal data used to make a decision about an individual. In particular to analyse a person's preferences, interests, behaviour, location or movements.
Right to erasure (to be forgotten): The right for data subjects to request their personal data to be erased 'without undue delay'.
Right to data portability: The right for data subjects to receive their personal data in a structured, commonly used and machine-readable format and to have it transferred to another data controller (e.g. when switching accounts).
Right to data subject access (SAR): The right for data subjects to ask a data controller to provide a copy (free of charge) of all the personal information being processed about them.
Sensitive Data or Special categories of data: Personal data about racial or ethnic origin; political opinions; religious or philosophical beliefs; trade-union membership; genetic data; biometric data; data concerning health or sex life; sexual orientation.
Sub Controller: The organisation that is appointed by a Data Processor to processes personal data on their behalf with the approval of the data controller.
Supervisory Authority: An independent public authority which is established by a Member State to enforce the data protection legislation; for us this is the ICO