Data Protection Policy

Version	Date	Reason for change	Authorised by
1.0	January 2018	Introduction	Chief Executive Jane Lockey

Author: Jane Lockey **Owner:** Louise Herbert **ReviewDate**: January 2020

CONTENTS		
1	Introduction to the General Data Protection Regulation	
2	Policy Scope	
3	Equal Opportunities	
4	Data Protection Principles	
5	Lawfulness of Processing	
6	The Rights of the Individual/Data Subject	
7	Consent	
8	Rights of Access to Data	
9	Retention & Disposal of Data	
10	Data Security	
11	Data Breach	
12	Policy & Performance Review	
13	Appendix A – Definition of Terms	

1. Introduction to the General Data Protection Regulation

1.1 The General Data Protection Regulation (GDPR) is a new, Europe-wide law that replaces the Data Protection Act 1998 in the UK. It is part of the wider package of reform to the data protection landscape that includes the Data Protection Bill. The GDPR sets out requirements for how organisations will need to handle personal data from 25 May 2018.

The GDPR applies to 'personal data', which means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier

1.2 Wessmaps Housing Trust (WHT) is committed to protecting the rights and privacy of individuals in accordance with the General Data Protection Regulation

In order for WHT to operate effectively, they have to collect, and process information about a range of people including, but not limited to, the following:

- tenants;

- employees (past and current members of staff and applicants);
- housing applicants;
- sharing owners;
- Board of Trustee members; and
- contractors/suppliers.

In order for WHT to comply with the law, information about individuals must be collected and used fairly, stored safely/securely and not disclosed to any third party unlawfully.

The GDPR applies to 'personal data' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.
This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way WHT collects information about people.

WHT may collect, process and store information such as:

- Tenant names, date of birth, National Insurance numbers, photographs, contact details and preferences
- Tenant demographic data (e.g. religion or belief, ethnicity)
- References from landlords, support providers or other people vouching for applicants' suitability as a tenant
- The details of other family members or people living in our properties
- Rent payments made
- Income and expenditure estimates
- Repairs requested
- Application or referral forms
- Tenancy agreements
- Physical and mental health or condition
- Support contracts
- Support plans and details of support providers
- Complaints about our services
- Responses to surveys or involvement initiatives
- Allegations of anti-social behaviour
- Convictions, proceedings and criminal acts
- Correspondence to and from our residents, service users, other agencies or advocates
- Recordings of telephone calls made to and from the organisation
- CCTV images (If you live in a supported accommodation project with the provision of CCTV; the CCTV systems record and retain information for up to a month to safeguard your health and security).

WHT may apply markers to this information (for example, in relation to a tenants vulnerability or health status) to enable us to tailor and deliver our services.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

The GDPR also refers to sensitive personal data as "special categories of personal data"

The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing

1.3 Failure to comply with the General Data Protection Regulation could result in the prosecution not only of a WHT member but also of the individual responsible for the breach in data security.

Data subjects (that is persons about whom such data is held) may also sue for compensation for damage and any associated distress suffered as a result of:

- loss or unauthorised destruction of data;
- unauthorised disclosure of, or access obtained to, data; and
- inaccurate data - i.e. data which is incorrect or misleading.

Financial penalties can be imposed on WHT members by the Information Commissioner for any serious breaches of the General Data Protection Regulation

1.4 Given the financial consequences of any serious breach of the General Data Protection Regulation, it is imperative that WHT staff, Board of Trustee Members or contractors concerned with, or having access to, such data ensure that data is processed according to the principles of data protection and the rights of data subjects.

WHT staff, Board of Trustee members and contractors must treat all data carefully and must not disclose any personal data to unauthorised persons (this includes parents or relatives of tenants or other data subjects).

2. Policy Scope

2.1 This policy applies to:

- all Wessmaps Housing Trust staff;
- all Board of Trustee members;
- contractors and suppliers appointed Wessmaps Housing Trust; and
- any bodies or organisations working with Wessmaps Housing Trust in a partnership/joint-working arrangement.

3. Equal Opportunities

3.1 WHT is committed to fairness and equality for all regardless of race, ethnicity, nationality (Gypsies, Travellers and white minority groups are included within these definitions), gender, sexual orientation, marital status, disability, state of health, age, beliefs or religion, appearance, family circumstances or criminal convictions.

WHT's key aim is to ensure that its' policies and procedures do not create an unfair disadvantage for anyone, directly or indirectly.

4. Data Protection Principles

4.1 When processing personal information, WHT will ensure that they comply at all times with the requirements of the General Data Protection Regulation. This compliance will ensure all personal information that is collected is processed fairly and for lawful purposes. This information will also be stored safely and not disclosed to any other person unlawfully.

The controller shall be responsible for and be able to demonstrate compliance.

In order to achieve the requirements, set out in 1.2, the WHT will comply in full with the principles contained in Article 5 of the General Data Protection Regulation in the following terms:

Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

e) 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

5. Lawfulness of Processing

5.1 Processing shall be lawful only if and to the extent that at least one of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(e) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(f) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(g) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

5.2 The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

(a) Union law; or

(b) Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

5.3 Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives, the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

(c) the nature of the personal data, in particular whether special categories of personal data are processed, or whether personal data related to criminal convictions and offences are processed;

(d) the possible consequences of the intended further processing for data subjects;

(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

6. The Rights of the Individual/Data Subject

6.1 The controller shall take appropriate measures to provide any information collected about the data subject and any communication relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

6.2 The controller shall facilitate the exercise of data subject rights, the controller shall not refuse to act on the request of the data subject for exercising his or her rights,

unless the controller demonstrates that it is not in a position to identify the data subject.

6.3 The controller shall provide information on action taken on a request without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. Where the data subject makes the request by electronic form means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

6.4 If the controller does not take action on the request of the data subject, the controller shall inform the data subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

6.5 Information provided, any communication and any actions taken shall be provided free of charge. Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either:

(a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

(b) refuse to act on the request.

The controller shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

6.6 Without prejudice, where the controller has reasonable doubts concerning the identity of the natural person making the request, the controller may request the provision of additional information necessary to confirm the identity of the data subject.

6.7 The information to be provided to data subjects may be provided in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.

6.8 The Commission shall be empowered to adopt delegated acts for the purpose of determining the information to be presented by the icons and the procedures for providing standardised icons.

7. Consent

7.1 Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

7.2 If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.

7.3 The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

7.4 When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

8. Rights of Access to Data

8.1 The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been

or will be disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with a supervisory authority;

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making, including profiling, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

8.2 Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant relating to the transfer.

8.3 The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

8.4 The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

9. Retention & Disposal of Data

9.1 The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant;

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services

9.2 Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

9.3 Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health;

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims.

10. Data Security

10.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(d) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(e) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

10.2 In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

10.3 Adherence to an approved code of conduct or an approved certification mechanism may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1.

10.4 The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

11. Data Breach

11.1 In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

11.2 The processor shall notify the controller without undue delay after becoming aware of a personal data breach.

11.3 The notification referred to in paragraph 1 shall at least:

(a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned, and the categories and approximate number of personal data records concerned;

(b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;

(c) describe the likely consequences of the personal data breach;

(d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

11.4 Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

11.5 The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.
2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article.
3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

(b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

(c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

12. Policy & Performance Review

This policy will be reviewed every two years, although ad hoc changes will be made to the policy during the three-year period if any the following occur:

• responding to any new legislative changes in the Data Protection Act; and

• to address any weaknesses in the policy that has been identified by a Group member as a result of a breach in data security.

Appendix A

Definition of Terms

Data Subject

This refers to any living individual who is the subject of personal data. Examples of data subjects for WHT are:

- Tenants, prospective tenants and former tenants
- Board of Trustee members
- Employees
- Sharing and factored owners
- Others in receipt of service
- Applicants seeking paid and non-paid employment with a Group member

Personal Data

Personal data relates to data that can identify an individual from information which is held by WHT. It also includes any expression of opinion or view about an individual or their circumstances.

Examples of personal data include, but not limited to, the following:

- Age
- Marital status
- Housing history
- Economic status
- Allowance, benefits and grants
- Support services received
- Medical data

Sensitive Personal Data

The GDPR refers to sensitive personal data as “special categories of personal data”

The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing.

The Act also recognises that some items of data are more sensitive than others and therefore require additional legislation to ensure appropriate handling.

Examples of sensitive personal data include, but are not limited, to the following:

- Race or ethnic origin
- Political opinions
- Religious or other beliefs
- Physical or mental health
- Criminal convictions