

EHS-UK LTD  
Data Protection Policy  
21/03/2026

## 1. Introduction

This Policy sets out the obligations of EHS-UK LTD a company registered in United Kingdom under number 17123544 whose registered office is at Endeavour House, Coopers End Road Stansted CM24 1SJ (“the Company”) regarding data protection and the rights of **landlords, tenants, prospective tenants, service users, clients, referral partners, business contacts, suppliers, contractors, employees and job applicants**

(“data subjects”) in respect of their personal data under Data Protection Law. “Data Protection Law” means all applicable legislation in force from time to time in the United Kingdom applicable to data protection and privacy including, but not limited to, the UK GDPR, the Data Protection Act 2018 (and regulations made thereunder), the Privacy and Electronic Communications Regulations 2003 as amended, the Data (Use and Access) Act 2025, and any successor legislation.

This Policy sets out the Company’s obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by the Company, its employees, agents, contractors, or other parties working on behalf of the Company.

## 2. Definitions

“ <b>automated decision-making</b> ”	means the making of a decision by automated means without meaningful human involvement;
“ <b>consent</b> ”	means the consent of the data subject which must be a freely given, specific, informed, and unambiguous indication of the data subject’s wishes by which they, by a statement or by a clear affirmative action, signify their agreement to the processing of personal data relating to them;
“ <b>data controller</b> ”	means the natural or legal person or organisation which, alone or jointly with others, determines the purposes and means of the processing of personal data. For the purposes of this Policy, the Company is the data controller of all personal data relating to <b>landlords, tenants, prospective tenants, service users, clients, referral partners, business contacts, suppliers, contractors, employees and job applicants</b>

<b>“data processor”</b>	in our business for our commercial purposes; means a natural or legal person or organisation which processes personal data on behalf of a data controller;
<b>[“The Director of EHS-UK Ltd”</b>	means the person appointed by the Company to oversee data protection compliance where the Company is not required to appoint a statutory Data Protection Officer;
<b>“data subject”</b>	means a living, identified, or identifiable natural person about whom the Company holds personal data;
<b>“EEA”</b>	means the European Economic Area, consisting of all EU Member States, Iceland, Liechtenstein, and Norway;
<b>“personal data”</b>	means any information relating to a data subject who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, 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 data subject;
<b>“personal data breach”</b>	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored, or otherwise processed;
<b>“processing”</b>	means any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
<b>“pseudonymisation”</b>	means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person; and
<b>“special category personal data”</b>	means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual life, sexual

orientation, biometric, or genetic data.

### 3. Scope

- 3.1 The Company is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.
- 3.2 The Company's -is Larna Joseph info@e-hs.org. TheThe Director of EHS-UK Ltd is responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.
- 3.3 All Landlords , Tenants , prospective tenants, service users ,clients suppliers, contractors,employees and job applicants are responsible for ensuring that all employees, agents, contractors, or other parties working on behalf of the Company comply with this Policy and, where applicable, must implement such practices, processes, controls, and training as are reasonably necessary to ensure such compliance.
- 3.4 Any questions relating to this Policy or to Data Protection Law should be referred to the The Director of EHS-UK Ltd. In particular, the The Director of EHS-UK Ltd should always be consulted in the following cases:
- a) if there is any uncertainty relating to the lawful basis on which personal data is to be collected, held, and/or processed;
  - b) if consent is being relied upon in order to collect, hold, and/or process personal data;
  - c) if there is any uncertainty relating to the retention period for any particular type(s) of personal data;
  - d) if any new or amended privacy notices or similar privacy-related documentation are required;
  - e) if any assistance is required in dealing with the exercise of a data subject's rights (including, but not limited to, the handling of subject access requests);
  - f) if a personal data breach (suspected or actual) has occurred;
  - g) if there is any uncertainty relating to security measures (whether technical or organisational) required to protect personal data;
  - h) if personal data is to be shared with third parties (whether such third parties are acting as data controllers or data processors);
  - i) if personal data is to be transferred outside of the UK and there are questions relating to the legal basis on which to do so;
  - j) when any significant new processing activity is to be carried out, or significant changes are to be made to existing processing activities, which will require a Data Protection Impact Assessment;
  - k) when personal data is to be used for purposes different to those for which it was originally collected;
  - l) if any automated processing, including profiling or automated decision-making, is to be carried out; or
  - m) if any assistance is required in complying with the law applicable to direct marketing; or

- n) if any data protection complaint is received from a data subject or someone acting on their behalf.

#### 4. **The Data Protection Principles**

This Policy aims to ensure compliance with Data Protection Law. The UK GDPR sets out the following principles with which any party handling personal data must comply. Data controllers are responsible for, and must be able to demonstrate, such compliance. All personal data must be:

- 4.1 processed lawfully, fairly, and in a transparent manner in relation to the data subject;
- 4.2 collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing must be assessed in accordance with Part 9 of this Policy. Further processing for archiving purposes in the public interest, scientific or historical research purposes (including qualifying commercial scientific research where permitted by Data Protection Law), or statistical purposes shall not be considered to be incompatible with the initial purposes;
- 4.3 adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed;
- 4.4 accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay;
- 4.5 kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is 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 (including qualifying commercial scientific research where permitted by Data Protection Law), or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of the data subject;
- 4.6 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.

#### 5. **The Rights of Data Subjects**

The UK GDPR sets out the following key rights applicable to data subjects:

- 5.1 The right to be informed;
- 5.2 the right of access;
- 5.3 the right to rectification;
- 5.4 the right to erasure (also known as the 'right to be forgotten');
- 5.5 the right to restrict processing;
- 5.6 the right to data portability;
- 5.7 the right to object; and

5.8 rights with respect to automated decision-making and profiling.

## 6. Lawful, Fair, and Transparent Data Processing

6.1 Data Protection Law seeks to ensure that personal data is processed lawfully, fairly, and transparently, without adversely affecting the rights of the data subject. Specifically, the processing of personal data shall be lawful if at least one of the following applies:

- a) the data subject has given consent to the processing of their personal data for one or more specific purposes;
- b) the processing is necessary for the performance of a contract to which the data subject is a party, or in order to take steps at the request of the data subject prior to entering into a contract;
- c) the processing is necessary for compliance with a legal obligation to which the data controller is subject;
- d) the processing is necessary to protect the vital interests of the data subject or of another natural person;
- e) the 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 data controller. (This lawful basis will not usually apply to private businesses unless they are carrying out a task in the public interest or exercising official authority under the law);
- f) the processing is necessary for the purposes of the legitimate interests pursued by the data controller or by a third party, except where such interests are overridden by the fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child; or
- g) where permitted by Data Protection Law, the Company may rely on a recognised legitimate interest. Recognised legitimate interests are limited to specific purposes set out in Data Protection Law and should not be treated as a general replacement for the ordinary legitimate interests lawful basis. Where the Company relies on a recognised legitimate interest, it shall record the relevant recognised legitimate interest and ensure that the processing is necessary for that purpose.

6.2 [If the personal data in question is special category personal data (also known as “sensitive personal data”), at least one of the following conditions must be met. Note that not all of the conditions listed below will be available to all organisations. In particular, conditions relating to public interest, public health, archiving in the public interest, or official functions should only be relied upon where they are applicable to the Company’s activities and supported by Data Protection Law:

- a) the data subject has given their explicit consent to the processing of such data for one or more specified purposes (unless the law prohibits them from doing so);
- b) the processing is necessary for the purpose of carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security, and social protection law (insofar as it is authorised by law or a collective agreement pursuant to law which provides for appropriate safeguards for the fundamental rights and interests of the data subject);

- c) the processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- d) the data controller is a foundation, association, or other non-profit body with a political, philosophical, religious, or trade union aim, and the processing is carried out in the course of its legitimate activities, provided that the processing relates solely to the members or former members of that body or to persons who have regular contact with it in connection with its purposes and that the personal data is not disclosed outside the body without the consent of the data subjects;
- e) the processing relates to personal data which is manifestly made public by the data subject;
- f) the processing is necessary for the conduct of legal claims or whenever courts are acting in their judicial capacity;
- g) the processing is necessary for substantial public interest reasons, on the basis of law which shall be proportionate to the aim pursued, shall respect the essence of the right to data protection, and shall provide for suitable and specific measures to safeguard the fundamental rights and interests of the data subject;
- h) the processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of an employee, for medical diagnosis, for the provision of health or social care or treatment, or the management of health or social care systems or services on the basis of law or pursuant to a contract with a health professional, subject to the conditions and safeguards referred to in Article 9(3) of the UK GDPR;
- i) the processing is necessary for public interest reasons in the area of public health, for example, protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject (in particular, professional secrecy); or
- j) the processing is necessary for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes in accordance with Article 89(1) of the UK GDPR (as supplemented by section 19 of the Data Protection Act 2018) based on law which shall be proportionate to the aim pursued, respect the essence of the right to data protection, and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

## 7. Consent

If consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, the following shall apply:

- 7.1 Consent is a clear indication by the data subject that they agree to the processing of their personal data. Such a clear indication may take the form of a statement or a positive action. Silence, pre-ticked boxes, or inactivity are unlikely to amount to consent.
- 7.2 Where consent is given in a document which includes other matters, the section

dealing with consent must be kept clearly separate from such other matters.

- 7.3 Data subjects are free to withdraw consent at any time and it must be made easy for them to do so. If a data subject withdraws consent, their request must be honoured promptly.
- 7.4 If personal data is to be processed for a new purpose, the Company must assess whether the new purpose is compatible with the original purpose, whether Data Protection Law otherwise permits the new processing, and whether a new lawful basis or updated privacy information is required. Where the new processing relies on consent and the original consent does not cover the new purpose, fresh consent must be obtained.
- 7.5 [If special category personal data is processed, the Company shall normally rely on a lawful basis other than explicit consent. If explicit consent is relied upon, the data subject in question must be issued with a suitable privacy notice in order to capture their consent.
- 7.6 In all cases where consent is relied upon as the lawful basis for collecting, holding, and/or processing personal data, records must be kept of all consents obtained in order to ensure that the Company can demonstrate its compliance with consent requirements.

## 8. Specified, Explicit, and Legitimate Purposes

- 8.1 The Company collects and processes the personal data set out in Part 25 of this Policy. This includes:
  - a) personal data collected directly from data subjects **OR** and
  - b) personal data obtained from third parties.
- 8.2 The Company only collects, processes, and holds personal data for the specific purposes set out in Part 25 of this Policy (or for other purposes expressly permitted by Data Protection Law).
- 8.3 Data subjects must be kept informed at all times of the purpose or purposes for which the Company uses their personal data. Please refer to Part 16 for more information on keeping data subjects informed.

## 9. Further Processing

- 9.1 The Company shall not process personal data for a new purpose that is incompatible with the purpose or purposes for which it was originally collected unless the data subject has given valid consent or the processing is otherwise permitted by Data Protection Law.
- 9.2 Before using personal data for a new purpose, the Company shall consider, where relevant:
  - a) any link between the original purpose and the new purpose;
  - b) the context in which the personal data was collected;
  - c) the nature of the personal data, including whether it includes special category personal data or criminal offence data;
  - d) the possible consequences of the new processing for data subjects; and
  - e) the existence of appropriate safeguards, including encryption or pseudonymisation, where appropriate.

- 9.3 Where Data Protection Law specifies that certain further processing is compatible with the original purpose, the Company may rely on that provision where applicable, provided that the processing is documented and appropriate safeguards are applied.
- 9.4 Where personal data is to be used for a new purpose, the Company shall update any and all applicable privacy information as required.

## 10. **Adequate, Relevant, and Limited Data Processing**

- 10.1 The Company will only collect and process personal data for and to the extent necessary for the specific purpose or purposes of which data subjects have been informed (or will be informed) as under Parts 8 and 9, above, and as set out in Part 25, below.
- 10.2 Employees, agents, contractors, or other parties working on behalf of the Company may collect personal data only to the extent required for the performance of their job duties and only in accordance with this Policy. Excessive personal data must not be collected.
- 10.3 Employees, agents, contractors, or other parties working on behalf of the Company may process personal data only when the performance of their job duties requires it. Personal data held by the Company cannot be processed for any unrelated reasons.

## 11. **Accuracy of Data and Keeping Data Up-to-Date**

- 11.1 The Company shall ensure that all personal data collected, processed, and held by it is kept accurate and up-to-date. This includes, but is not limited to, the rectification of personal data at the request of a data subject, as set out in Part 18, below.
- 11.2 The accuracy of personal data shall be checked when it is collected and at regular **OR** Annually intervals thereafter. If any personal data is found to be inaccurate or out-of-date, all reasonable steps will be taken without delay to amend or erase that data, as appropriate.

## 12. **Data Retention**

- 12.1 The Company shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed.
- 12.2 When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.
- 12.3 For full details of the Company's approach to data retention, including retention periods for specific personal data types held by the Company, please refer to our Data Retention Policy.

## 13. **Secure Processing**

- 13.1 The Company shall ensure that all personal data collected, held, and processed is kept secure and protected against unauthorised or unlawful processing and against accidental loss, destruction, or damage. Further details of the technical and organisational measures which shall be taken are provided in Parts 26 to

31 of this Policy.

- 13.2 All technical and organisational measures taken to protect personal data shall be regularly reviewed and evaluated to ensure their ongoing effectiveness and the continued security of personal data.
- 13.3 Data security must be maintained at all times by protecting the confidentiality, integrity, and availability of all personal data as follows:
  - a) only those with a genuine need to access and use personal data and who are authorised to do so may access and use it;
  - b) personal data must be accurate and suitable for the purpose or purposes for which it is collected, held, and processed; and
  - c) authorised users must always be able to access the personal data as required for the authorised purpose or purposes.

#### 14. **Accountability and Record-Keeping**

- 14.1 The The Director of EHS-UK Ltd **is** responsible for administering this Policy and for developing and implementing any applicable related policies, procedures, and/or guidelines.
- 14.2 The Company shall follow a privacy by design approach at all times when collecting, holding, and processing personal data. Data Protection Impact Assessments shall be conducted if any processing is likely to result in a high risk to the rights and freedoms of data subjects (please refer to Part 15 for further information).
- 14.3 All employees, agents, contractors, or other parties working on behalf of the Company shall be given appropriate training in data protection and privacy, addressing the relevant aspects of Data Protection Law, this Policy, and all other applicable Company policies.
- 14.4 The Company's data protection compliance shall be regularly reviewed and evaluated by means of Data Protection Audits.
- 14.5 The Company shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:
  - a) the name and details of the Company, its The Director of EHS-UK Ltd, and any applicable third-party data transfers (including data processors and other data controllers with whom personal data is shared);
  - b) the purposes for which the Company collects, holds, and processes personal data;
  - c) the Company's lawful basis or bases for collecting, holding, and processing personal data, including, where applicable, details of any consent relied upon, the mechanism(s) for obtaining such consent, and records of such consent, details of any ordinary legitimate interests relied upon and any legitimate interests assessment, and details of any recognised legitimate interest relied upon;
  - d) details of the categories of personal data collected, held, and processed by the Company, and the categories of data subject to which that personal data relates;
  - e) details of any transfers of personal data to non-UK countries including all mechanisms and security safeguards;

- f) details of how long personal data will be retained by the Company (please refer to the Company's Data Retention Policy);
- g) details of personal data storage, including location(s);
- h) detailed descriptions of all technical and organisational measures taken by the Company to ensure the security of personal data;
- i) where applicable, details of any further processing compatibility assessments; and
- j) records of data protection complaints received, the steps taken to investigate and respond to them, and any remedial action taken.

## 15. **Data Protection Impact Assessments and Privacy by Design**

- 15.1 In accordance with the privacy by design principles, the Company shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and where the processing involved is likely to result in a high risk to the rights and freedoms of data subjects.
- 15.2 The principles of privacy by design should be followed at all times when collecting, holding, and processing personal data. The following factors should be taken into consideration:
- a) the nature, scope, context, and purpose or purposes of the collection, holding, and processing;
  - b) the state of the art of all relevant technical and organisational measures to be taken;
  - c) the cost of implementing such measures; and
  - d) the risks posed to data subjects and to the Company, including their likelihood and severity.
- 15.3 Data Protection Impact Assessments shall be overseen by the The Director of EHS-UK Ltd and shall address the following:
- a) the type(s) of personal data that will be collected, held, and processed;
  - b) the purpose(s) for which personal data is to be used;
  - c) the Company's objectives;
  - d) how personal data is to be used;
  - e) the parties (internal and/or external) who are to be consulted;
  - f) the necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
  - g) risks posed to data subjects;
  - h) risks posed both within and to the Company; and
  - i) proposed measures to minimise and handle identified risks.

## 16. **Keeping Data Subjects Informed**

- 16.1 The Company shall provide the information set out in Part 16.2 to every data subject:

- a) where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and
- b) where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:
  - i) if the personal data is used to communicate with the data subject, when the first communication is made; or
  - ii) if the personal data is to be transferred to another party, before that transfer is made; or
  - iii) as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

16.2 The following information shall be provided in the form of a privacy notice:

- a) details of the Company including, but not limited to, contact details, and the names and contact details of any applicable representatives and its The Director of EHS-UK Ltd,
- b) the purpose(s) for which the personal data is being collected and will be processed (as detailed in Part 25 of this Policy) and the lawful basis justifying that collection and processing;
- c) where processing is based on the legitimate interests lawful basis, details of the legitimate interests relied upon by the Company or by a third party, and where processing is based on recognised legitimate interests, details of the recognised legitimate interest relied upon;
- d) where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;
- e) where the personal data is to be transferred to one or more third parties, details of those parties;
- f) where the personal data is to be transferred to a third party that is located outside of the UK, details of that transfer, including but not limited to the safeguards in place (see Part 32 of this Policy for further details);
- g) details of applicable data retention periods;
- h) details of the data subject's rights under the UK GDPR;
- i) details of the data subject's right to withdraw their consent to the Company's processing of their personal data at any time;
- j) details of how the data subject can raise a data protection complaint with the Company, including how such a complaint can be submitted electronically, and details of the data subject's right to complain to the Information Commissioner's Office;
- k) where the personal data is not obtained directly from the data subject, details about the source of that personal data;
- l) where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and
- m) where applicable, details of any solely automated decision-making, including profiling, that will have legal or similarly significant effects on data subjects, meaningful information about the logic involved, the significance and envisaged consequences of such processing, and the safeguards available to data subjects.

## 17. **Data Subject Access**

- 17.1 Data subjects may make subject access requests (“SARs”) at any time to find out more about the personal data which the Company holds about them, what it is doing with that personal data, and why.
- 17.2 When responding to a SAR, the Company shall carry out reasonable and proportionate searches for the personal data requested, taking into account the nature of the request, the personal data likely to be held, the systems and records used by the Company, and the effort involved in locating the relevant personal data.
- 17.3 If the Company reasonably requires clarification in order to respond to a SAR, it may request clarification from the data subject. Where permitted by Data Protection Law, the time limit for responding to the SAR shall be paused until the data subject provides the clarification requested. The Company shall only request clarification where it is reasonably necessary and shall record the request, the reason for it, and the date on which clarification is received.
- 17.4 [Employees wishing to make a SAR are encouraged to use the Company’s Subject Access Request Form, and send it to the The Director of EHS-UK Ltd at info@e-hs.org The Company shall not refuse to handle a SAR solely because it has not been submitted using that form.
- 17.5 Responses to SARs must normally be made within one month of receipt, however, this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.
- 17.6 All SARs received shall be handled by theThe Director of EHS-UK Ltd and in accordance with the Company’s Data Subject Access Request Policy & Procedure.
- 17.7 The Company does not charge a fee for the handling of normal SARs. The Company reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

## 18. **Rectification of Personal Data**

- 18.1 Data subjects have the right to require the Company to rectify any of their personal data that is inaccurate or incomplete.
- 18.2 The Company shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing the Company of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.
- 18.3 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

## 19. **Erasure of Personal Data**

- 19.1 Data subjects have the right to request that the Company erases the personal

data it holds about them in the following circumstances:

- a) it is no longer necessary for the Company to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;
- b) the data subject wishes to withdraw their consent to the Company holding and processing their personal data;
- c) the data subject objects to the Company holding and processing their personal data (and there is no overriding legitimate interest to allow the Company to continue doing so) (see Part 22 of this Policy for further details concerning the right to object);
- d) the personal data has been processed unlawfully;
- e) the personal data needs to be erased in order for the Company to comply with a particular legal obligation;
- f) the personal data is being held and processed for the purpose of providing information society services to a child.

19.2 Unless the Company has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

19.3 In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

## 20. **Restriction of Personal Data Processing**

20.1 Data subjects may request that the Company ceases processing the personal data it holds about them. If a data subject makes such a request, the Company shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

20.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

## 21. **[Data Portability**

21.1 The Company processes personal data using - Electronic systems including emails , cloud based storage systems, property management software, CRM systems and accounting software.

21.2 Where data subjects have given their consent to the Company to process their personal data in such a manner, or the processing is otherwise required for the performance of a contract between the Company and the data subject, data subjects have the right, under the UK GDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).

21.3 To facilitate the right of data portability, the Company shall make available all applicable personal data to data subjects in the following format :

a) PDF, Microsoft Word (DOCX) , Microsoft Excel (XLSX) and CSV

21.4 Where technically feasible, if requested by a data subject, personal data shall be sent directly to the required data controller.

21.5 All requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

## 22. **Objections to Personal Data Processing**

22.1 Data subjects have the right to object to the Company processing their personal data based on ordinary legitimate interests, for direct marketing (including profiling),

22.2 Where a data subject objects to the Company processing their personal data based on ordinary legitimate interests, the Company shall cease such processing unless it can demonstrate compelling legitimate grounds for such processing which override the data subject's interests, rights, and freedoms, or that the processing is necessary for the establishment, exercise, or defence of legal claims.

22.3 Where the Company relies on a recognised legitimate interest, any objection shall be considered in accordance with Data Protection Law and the specific recognised legitimate interest relied upon.

22.4 Where a data subject objects to the Company processing their personal data for direct marketing purposes, the Company shall cease such processing promptly.

22.5 [Where a data subject objects to the Company processing their personal data for scientific and/or historical research and statistics purposes, the data subject must, under the UK GDPR, demonstrate grounds relating to his or her particular situation. The Company is not required to comply if the research is necessary for the performance of a task carried out for reasons of public interest.]

## 23. **[Automated Processing, Automated Decision-Making, and Profiling**

23.1 EHS-UK Ltd does not use personal data for automated decision-making

23.2 EHS -UK Ltd does not use personal data for profiling purposes. All decisions relating to accommodation, referrals, property , management and support services involve human review and are not based solely on automated processing.

23.3 Where the Company carries out solely automated decision-making, including profiling, that produces legal effects concerning a data subject or similarly significant effects, it shall ensure that:

- a) there is a valid lawful basis for the processing;
  - b) the processing is fair, transparent, necessary, and proportionate;
  - c) the data subject is provided with clear information about the processing;
- and

- d) appropriate safeguards are in place.
- 23.4 The safeguards referred to in Part 23.3(d) shall include measures enabling the data subject to:
- a) make representations about the decision;
  - b) obtain human intervention; and
  - c) contest the decision.
- 23.5 Where special category personal data is used for solely automated decision-making that produces legal or similarly significant effects, the Company shall only carry out such processing where permitted by Data Protection Law and subject to any additional safeguards required.
- 23.6 The Company shall not use automated decision-making or profiling in a way that results in unlawful discrimination or otherwise breaches Data Protection Law.
- 23.7 When personal data is used for automated processing, automated decision-making, or profiling, the Company shall implement appropriate technical and organisational measures to minimise the risk of errors, enable errors to be corrected, and secure the personal data against unauthorised or unlawful processing (see Parts 26 to 31 of this Policy for more details on data security and organisational measures).

## 24. **Direct Marketing**

- 24.1 The Company is subject to certain rules and regulations when marketing its accommodation services and housing solutions.
- 24.2 The prior consent of data subjects is required for electronic direct marketing including email, text messaging, and automated telephone calls, subject to the following limited exception:
- a) The Company may send marketing text messages or emails to a customer provided that that customer's contact details have been obtained in the course of a sale, the marketing relates to similar products or services, and the customer has been given the opportunity to opt out of marketing when their details were first collected and in every subsequent communication from the Company.
- 24.3 The Company shall comply with Data Protection Law when carrying out direct marketing and when using cookies, pixels, tracking technologies, or similar storage and access technologies.
- 24.4 The right to object to direct marketing shall be explicitly offered to data subjects in a clear and intelligible manner and must be kept separate from other information in order to preserve its clarity.
- 24.5 If a data subject objects to direct marketing, their request must be complied with promptly. A limited amount of personal data may be retained in such circumstances to the extent required to ensure that the data subject's marketing preferences continue to be complied with.]

## 25. **Personal Data Collected, Held, and Processed**

The following personal data is collected, held, and processed by the Company (for details of data retention, please refer to the Company's Data Retention Policy):

<b>Data Ref.</b>	<b>Type of Data</b>	<b>Purpose of Data</b>
PD001	Name, address, date of birth and contact details	Identity verification and tenancy management
PD02	Email address and telephone number	Communication with applicants, tenants, landlords and partners
PD03	Employment , income and affordability information	Assessing accommodation suitability and contractual arrangements
PD04	Emergency contact information	Safeguarding and welfare purposes
PD05	Landlord , property owner and agent details	Property management and contractual obligations
PD06	Referral information from local authorities, charities and support organisations	Housing placement and support coordination
PD07	Property inspection records and tenancy records	Compliance, property management and audit purposes
PD08	Financial and payment information	Rent collection , invoicing and accounting requirements

## 26. **Data Security - Transferring Personal Data and Communications**

The Company shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

- 26.1 All emails containing personal data must be encrypted using Microsoft 365 email security controls, password-protected documents where appropriate, and secure cloud-base storage systems.
- 26.2 All emails containing personal data must be marked “confidential”;
- 26.3 Personal data may only be transmitted using secure methods appropriate to the nature and sensitivity of the personal data, including secure networks, encrypted communications, secure file transfer systems, access-controlled portals, or other approved methods;
- 26.4 Wireless networks may be used to transmit personal data only where appropriate security measures are in place, such as encryption, password protection, and access controls;
- 26.5 Personal data contained in emails or messaging systems must be handled in accordance with the Company’s retention, security, and acceptable use policies. Where personal data is copied to another system of record, unnecessary duplicate copies should be deleted where appropriate;
- 26.6 Where personal data is to be sent by facsimile transmission the recipient should

be informed in advance of the transmission and should be waiting by the fax machine to receive the data;

- 26.7 Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient Royal Mail signed for, Royal Mail Special Delivery, or other tracked and secure courier services.
- 26.8 All personal data to be transferred physically, whether in hardcopy form or on removable electronic media shall be transferred in a suitable container marked "confidential";
- 26.9 Access to personal data is restricted to authorised personnel only. User accounts are protected by strong passwords and multi-factor authentication where available.

## 27. **Data Security - Storage**

The Company shall ensure that the following measures are taken with respect to the storage of personal data:

- 27.1 All electronic copies of personal data should be stored securely using passwords and industry-standard encryption and password protection.
- 27.2 All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;
- 27.3 All personal data stored electronically should be backed up daily using secure cloud-based backup systems. All backups should be encrypted using industry-standard encryption.
- 27.4 No personal data should be stored on any mobile device (including, but not limited to, laptops, tablets, and smartphones), whether such device belongs to the Company or otherwise [without the formal written approval of without the formal written approval of the Director of EHS-UK Ltd and, in the event of such approval, strictly in accordance with all instructions and limitations described at the time the approval is given, and for no longer than is absolutely necessary];
- 27.5 No personal data should be transferred to any device personally belonging to an employee, agent, contractor, or other party working on behalf of the Company and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of the Company where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the applicable Data Protection Law (which may include demonstrating to the Company that all suitable technical and organisational measures have been taken);
- 27.6 Personal data shall only be accessed where necessary for legitimate business purposes and in accordance with this policy.

## 28. **Data Security - Disposal**

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of. For further information on the deletion and disposal of personal data, please refer to the Company's Data Retention Policy.

## 29. **Data Security - Use of Personal Data**

The Company shall ensure that the following measures are taken with respect to the use of personal data:

- 29.1 No personal data may be shared informally and if an employee, agent, contractor, or other party working on behalf of the Company requires access to any personal data that they do not already have access to, such access should be formally requested from the Director of EHS-UK Ltd;
- 29.2 No personal data may be transferred to any employee, agent, contractor, or other party, whether such parties are working on behalf of the Company or not, without the authorisation of the Director of EHS-UK Ltd;
- 29.3 Personal data must not be entered into AI tools, generative AI systems, or other third-party platforms unless the use has been approved by the Director of EHS-UK Ltd and appropriate data protection safeguards are in place;
- 29.4 Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, contractors, or other parties at any time;
- 29.5 If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it;
- 29.6 Where personal data held by the Company is used for marketing purposes, it shall be the responsibility of Director to ensure that the appropriate consent is obtained and that no data subjects have opted out, whether directly or via a third-party service such as the TPS;
- 29.7 All employees , contractors and agents must report any actual or suspected data breach immediately to the Director of EHS-UK Ltd.

## 30. **Data Security - IT Security**

The Company shall ensure that the following measures are taken with respect to IT and information security:

- 30.1 All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All passwords must contain a combination of uppercase and lowercase letters, numbers, and symbols. [All software used by the Company is designed to require such passwords.];
- 30.2 Under no circumstances should any passwords be written down or shared between any employees, agents, contractors, or other parties working on behalf of the Company, irrespective of seniority or department. If a password is forgotten, it must be reset using the applicable method. IT staff do not have access to passwords;
- 30.3 All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. The Company's IT staff shall be responsible for installing any and all security-related updates not more than 14 Days after the updates are made available by the publisher or manufacturer soon as reasonably and practically possible, unless there are valid technical reasons not to do so;
- 30.4 No software may be installed on any Company-owned computer or device without the prior approval of the Director of EHS-UK Ltd;

- 30.5 Anti virus software, firewall protection and malware detection software shall be maintained on all Company-owned devices where applicable.

### 31. Organisational Measures

The Company shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

- 31.1 All employees, agents, contractors, or other parties working on behalf of the Company shall be made fully aware of both their individual responsibilities and the Company's responsibilities under Data Protection Law and under this Policy, and shall be provided with a copy of this Policy;
- 31.2 Only employees, agents, contractors, or other parties working on behalf of the Company that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by the Company;
- 31.3 All sharing of personal data shall comply with the information provided to the relevant data subjects and, if required, the consent of such data subjects shall be obtained prior to the sharing of their personal data;
- 31.4 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately trained to do so;
- 31.5 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be appropriately supervised;
- 31.6 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;
- 31.7 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;
- 31.8 All personal data held by the Company shall be reviewed periodically, as set out in the Company's Data Retention Policy;
- 31.9 The performance of those employees, agents, contractors, or other parties working on behalf of the Company handling personal data shall be regularly evaluated and reviewed;
- 31.10 All employees, agents, contractors, or other parties working on behalf of the Company handling personal data will be bound to do so in accordance with the principles of Data Protection Law and this Policy by contract;
- 31.11 All agents, contractors, or other parties working on behalf of the Company handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of the Company arising out of this Policy and Data Protection Law;
- 31.12 Where any agent, contractor or other party working on behalf of the Company handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless the Company against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure;
- 31.13 All staff, contractors and agents handling personal data shall receive appropriate data protection and information security training relevant to their role.

## 32. **Transferring Personal Data to a Country Outside the UK**

- 32.1 The Company may, from time to time, transfer personal data, including by making it available remotely, to countries or organisations outside of the UK. The Company shall only do so where Data Protection Law permits the transfer and where the level of protection for data subjects is not undermined.
- 32.2 Personal data may only be transferred to a country outside the UK if one of the following applies:
- a) The UK has issued adequacy regulations confirming that the personal data will receive an adequate level of protection (referred to as 'adequacy decisions', 'adequacy regulations', or 'partial findings of adequacy'). Such regulations may apply to a country as a whole, organisation(s), framework(s) or mechanism(s), or to data covered by specific legislation. Since 1 January 2021, transfers of personal data from the UK to EEA countries have continued to be permitted. Pre-existing EU Commission adequacy decisions in effect as at 31 December 2020 are also recognised, subject to ongoing review by the UK Government.
  - b) Appropriate safeguards are in place including binding corporate rules, standard contractual clauses approved for use in the UK, an approved code of conduct, or an approved certification mechanism. Standard contractual clauses include the International Data Transfer Agreement issued by the Information Commissioner's Office and the International Data Transfer Addendum to the current EU Commission Standard Contractual Clauses (set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021), issued by the Information Commissioner's Office. Where appropriate safeguards are relied upon, the Company shall carry out and document any transfer risk assessment required by Data Protection Law, taking into account whether the standard of protection for the personal data will be materially lower than that provided under UK Data Protection Law.
  - c) The transfer is made with the informed and explicit consent of the relevant data subject(s).
  - d) The transfer is necessary for one of the other reasons set out in the UK GDPR including the performance of a contract between the data subject and the Company; public interest reasons; for the establishment, exercise, or defence of legal claims; to protect the vital interests of the data subject where the data subject is physically or legally incapable of giving consent; or, in limited circumstances, for the Company's legitimate interests.

## 33. **Data Protection Complaints**

- 33.1 Data subjects may submit complaints about the Company's handling of their personal data or compliance with Data Protection Law by contacting the Director of EHS-UK Ltd or by using email [info@e-hs.org](mailto:info@e-hs.org).
- 33.2 The Company shall take appropriate steps to make it easy for data subjects to submit data protection complaints, including by electronic means.
- 33.3 The Company shall acknowledge receipt of a data protection complaint within 30 days of receipt.

- 33.4 The Company shall consider the complaint without undue delay and shall provide a response to the complainant within a reasonable period.
- 33.5 If the Company requires further information in order to investigate the complaint, it shall request that information promptly.
- 33.6 The Company shall keep records of data protection complaints received, the steps taken to investigate them, the outcome, and any remedial action taken.
- 33.7 Data subjects remain entitled to complain to the Information Commissioner's Office.

**34. Data Breach Notification**

- 34.1 All personal data breaches must be reported immediately to the Company's Director of EHS-UK Ltd.
- 34.2 If an employee, agent, contractor, or other party working on behalf of the Company becomes aware of or suspects that a personal data breach has occurred, they must not attempt to investigate it themselves. Any and all evidence relating to the personal data breach in question should be carefully retained.
- 34.3 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Director of EHS-UK must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.
- 34.4 In the event that a personal data breach is likely to result in a high risk (that is, a higher risk than that described under Part 34.3) to the rights and freedoms of data subjects, the Director of EHS-UK Ltd must ensure that all affected data subjects are informed of the breach directly and without undue delay.
- 34.5 Data breach notifications shall include the following information:
  - a) The categories and approximate number of data subjects concerned;
  - b) The categories and approximate number of personal data records concerned;
  - c) The name and contact details of the Company's Director of EHS-UK Ltd (or other contact point where more information can be obtained);
  - d) The likely consequences of the breach;
  - e) Details of the measures taken, or proposed to be taken, by the Company to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

**35. Implementation of Policy**

This Policy shall be deemed effective as of 21/03/2026. No part of this Policy shall have retroactive effect and shall thus apply only to matters occurring on or after this date.

This Policy has been approved and authorised by:

**Name:** Larna Joseph

**Position:** Director

**Date:** 21/03/2026

**Due for Review by:** 21/03/2027

**Signature:**

A handwritten signature in black ink, appearing to read 'L. Joseph' or similar, written in a cursive style.