Record Keeping Policy

1. Introduction

1.1. This Record Keeping Policy is TenderHelp Ltd.'s (hereafter referred to as "us", "we", or "our") policy regarding the safekeeping of all records from their creation to disposal – this includes our procedures for sharing information externally.

2. Purpose

2.1. This policy will ensure that records are properly created, accessible and available for use and that they are disposed of in a secure and timely fashion. It provides staff with guidance regarding individual responsibility for accuracy and appropriate storage of records.

2.2. This Record Keeping Policy covers:

2.2.1. Our record keeping procedure from creation to disposal;

2.2.2. Transparency procedures;

2.2.3. Our retention & disposal procedures;

2.2.4. Our information handling procedures – including our procedures for safely and legally sharing information externally;

2.2.5. Procedures for individuals making requests about their data (GDPR individual data rights);

2.2.6. Subject access request procedures;

2.2.7. Right to erasure ('Right to be forgotten') procedures;

2.2.8. Right to restrict processing procedures;

2.2.9. Right to object procedures;

2.2.10. Our procedures when there is a withdrawal of consent to share.

3. Scope

3.1. This policy includes in its scope all data which we process either in hardcopy or digital copy, this includes special categories of data.

3.2. This policy applies to all staff, including temporary staff and contractors.

4. Record keeping procedures – creation and use of records

4.1. When we create records, we use standardised structures and layouts for the contents of records.

4.2. All records are kept in accessible but protected locations. The location of these records is documented in the Information Asset Register (IAR). The security procedures around access to records are detailed in the Data Security Policy.

4.3. Throughout the lifespan of the record we:

- 4.3.1. Provide staff with guidance and training on the creation and use of records and their legal responsibilities to share and safeguard personal confidential information;
- 4.3.2. Monitor access to the record. The procedures which detail our auditing and monitoring process are detailed in our Data Security Policy.

4.4. At any point in the lifespan of the record, the data subject has the right to request access to their data. These subject access procedures are detailed in [9].

4.5. At any point in the lifespan of the record, the data subject has the right to request that their record is corrected. These procedures are detailed in the Data Quality Policy.

4.6. At any point in the lifespan of the record, the data subject has the right to request the erasure ('Right to be forgotten') of their record. These procedures are outlined in [10].

4.7. Records are only retained while they are necessary for the purposes for which they were originally collected. We will ensure that all records are retained and destroyed in-line with [6] Retention & Disposal Procedures.

4.8. At least annually we guarantee that we will audit our record keeping procedures to ensure that they are adequate and continue to keep our records to the highest standards.

5. Transparency procedures

5.1. Our privacy notice outlines to people why we hold their data, the lawful basis for doing so, and their rights in terms of how we process their data.

5.2. Our privacy notice is freely available to all individuals whose data we process and is part of our commitment to transparency and accountability. It satisfies the individual's right to be informed under GDPR.

5.3. All individuals are informed of their rights regarding their personal data.

5.4. The privacy notice will be reviewed and updated at least annually.

5.5. The privacy notice has been signed off by our Managing Director and DPO, Kyle Jameson.

5.6. We will provide people with this information at the moment that we ask them to give us their personal data.

5.7. If we receive an individual's personal data from a source other than that individual, we will provide them with privacy information without undue delay and at least within one month.

6. Retention schedule & disposal procedures

6.1. At the end of their lifespan, the records will go through an appraisal process. This process will determine if there is a continuing legal basis for keeping the record. Kyle Jameson will have final responsibility for determining whether the record will be destroyed or retained. They will maintain a record of all retention or disposal decisions.

6.2. In the instance that records are destroyed, our in-house process is in compliance with the British Security Industry Association EN 15713:2009 standard.

6.3. If we use a third-party contractor to dispose of records, we will ensure we have a written contract which specifies that they comply with this standard.

7. Information handling procedures

7.1. Information Handling Procedures ensure that personal information is protected and that it is not disclosed inappropriately, either by accident or design, whilst in use or when it is being transferred.

7.2. In line with legislation, personal information is not processed without a lawful basis being identified. The Record of Processing Activities (ROPA) records all processing of personal data and identifies the legal basis for it being processed.

7.3. These procedures cover all records which contain data or information which can be said to contain personal data whether stored in hardcopy or digitally.

7.4. Guidelines for staff on the secure use of personal information are outlined in the staff handbook and staff code of confidentiality.

7.5. We ensure that there are secure points for the receipt of personal information transferred to us and we have applied the following measures to safeguard personal information during receipt and transfer/transit:

7.5.1. Verbal communications:

7.5.1.1. Staff members have been provided with training on verbal communications. They know that they must take appropriate precautions not to reveal confidential information e.g. to avoid being overheard when making a phone call or not to have confidential conversations in public places or open offices. The staff handbook and their training inform them that breach of this procedure may be a disciplinary or legal offense.

7.5.2. Postal services and couriers:

7.5.2.1. We will ensure that all confidential information we transfer by post or courier is done so as securely as is practicable. All records transferred in this manner are addressed to a named individual and

marked “Private and Confidential”. All records which are posted will be done through signed-for delivery so that it is guaranteed that the correct person receives the record.

7.5.3. Portable devices:

We recognise that information held on portable devices is at increased risk. Portable devices include memory sticks, CDs, DVDs, mobile phones etc. All portable devices have been documented on the IAR, and all relevant staff have received guidelines on safe usage and have signed a Portable Device Assignment Form.

7.5.3.1. Portable devices must be encrypted;

7.5.3.2. Only portable devices issued by us may be used;

7.5.3.3. Portable devices such as memory sticks, CDs, etc. must not be used on personal computers;

7.5.3.4. All portable devices are security marked;

7.5.3.5. Password protected screensavers are installed on laptops;

7.5.3.6. Anti-virus software is in use and is regularly updated. This patching schedule is detailed in the Network Security Policy;

7.5.3.7. Regular backups are taken of the data stored on portable devices;

7.5.3.8. All portable devices are protected by either a PIN or password (dependent on the type of device).

7.5.4. Faxes:

The fax machine is in our main office and when receiving faxes containing confidential information, the organisation ensures:

7.5.4.1. The fax machine is located in secure area.

7.5.4.2. The fax is removed from the machine as soon as it is received;

7.5.4.3. Where necessary, the sender is contacted to confirm receipt;

7.5.4.4. The information in the fax is appropriately dealt with and safely stored.

To ensure that confidential information transferred from the organisation by fax is done so as securely as is practicable, the organisation ensures:

7.5.4.5. The fax number is always double checked, and frequently used numbers are stored in the fax machine to reduce the risk of typing errors;

7.5.4.6. A fax cover sheet is used and marked "Private and Confidential";

7.5.4.7. Faxes are only sent to a named person rather than a team;

7.5.4.8. The recipient is informed that a fax will be sent, and asked to confirm receipt;

7.5.4.9. Faxes are not sent outside a recipient organisation's working hours where there is no-one present to receive;

7.5.4.10. We regularly check the date and time, especially following power outages, or change of British summer time;

7.5.4.11. Journal logs are retained in line with our retention schedule.

7.5.5. Email:

7.5.5.1. We undertake that person identifiable information (either of employees or service users) can only be sent by secure email. Both the recipient and sender must have access to secure email.

7.5.6. Other forms of information exchange (e.g. text messages, upload through online portals etc.)

8. Procedures for individual's making requests about their data (GDPR individual data rights)

8.1. GDPR provides all individuals within the EU specific rights when it comes to their personal data.

8.2. To exercise these rights an individual should contact any staff member, though ideally the Data Protection Champion, and make a request either verbally or in writing.

8.3. In the instance that the request is made to a member of staff who is not the Data Protection Champion, that staff member will inform the Data Protection Champion as soon as possible, the timeline for responding to requests begins from when the first staff member is contacted.

8.4. In all cases we will respond to a request without delay and in a timeframe not exceeding one month from when the request was made.

8.5. Should the request be complex this may be extended to two months, however, we will inform the individual in writing of the extension and the reasons why it is required within one month.

8.6. If the request is manifestly unfounded or excessive, we may either request a reasonable fee to cover our administrative costs or we may refuse to comply with the request.

8.7. If we refuse to comply with a request, we will inform the individual why we are not taking action, tell them about their right to complain to the ICO, and tell them that they have the right to seek a judicial remedy.

8.8. In order to process any request, we will use reasonable means to verify the identity of the individual making the request so that no data is shared inappropriately.

8.9. The Data Protection Champion will maintain a log of all requests and their outcomes.

8.10. All staff will be informed of these procedures in the staff handbook.

9. Subject access request procedures

9.1. All individuals have the right to access their personal data which we process and store.

9.2. Confidential records of the deceased have the rights afforded to them by the Duty of Confidentiality and the Access to Health Records Act 1990. Should any person wish to request access for any records of the deceased they should contact the Data Protection Champion.

9.3. We will provide a copy of any information which it is lawful to provide free of charge. If further copies are required, we will charge a fee which will exclusively cover the administration costs of making copies.

9.4. We will provide copies of the information requested in a reasonable format – either in hard copy or digital.

10. Right to erasure procedures

10.1. All citizens have the right to request the erasure of their data which we control or process.

10.2. Citizens can request for their data to be erased in the following instances:

10.2.1. Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed;

10.2.2. When they withdraw consent;

10.2.3. When they object to the processing and there is no overriding legitimate interest for continuing the processing;

10.2.4. The personal data was unlawfully processed;

10.2.5. The personal data must be erased in order to comply with a legal obligation;

10.2.6. The personal data is processed in relation to the offer of information society services to a child.

10.3. We will not be able to honour any requests to have personal data erased when the data is being processed for the following reasons:

10.3.1. to assess the working capacity of an employee;

10.3.2. to exercise the right of freedom of expression and information;

10.3.3. to comply with a legal obligation for the performance of a public interest task or exercise of official authority;

10.3.4. for public health purposes in the public interest;

10.3.5. archiving purposes in the public interest, scientific research historical research or statistical purposes;

10.3.6. the exercise or defence of legal claims.

10.4. Where at all possible, in the instance that we have appropriately shared an individual's records with any third-party we will inform this third-party of the erasure if appropriate.

10.5. We will erase records in line with the disposal procedures set out above.

11. Right to restrict processing procedures

11.1. All individuals have the right to request that we restrict the processing of their data in the following circumstances:

11.1.1. while we are verifying the accuracy of any data we keep when an individual has made a request for the rectification of their personal data;

11.1.2. in the instance that their personal data has been processed unlawfully and the individual requests that their data is not erased;

11.1.3. When we do not need to keep the personal data but the individual has requested that we keep it in order to establish, exercise or defend a legal claim;

11.1.4. If an individual objects to us processing their personal data, we will restrict all processing while we investigate the request.

11.2. When we restrict processing, we will store the individual's personal data but will not process their data in any other way.

12. Right to object procedures

12.1. All people have the right to object to us processing their data in the certain circumstances.

12.2. They have an absolute right to object to us using their personal data for any direct marketing.

12.3. If they object to us using their data for marketing, we will immediately stop using their data for this purpose. We will retain only enough data for us to be able to have a record that they don't want to receive direct marketing so that their request can be respected.

12.4. Individuals can also object to us processing their data if we are doing it under Public Task or Legitimate Interests grounds. The individual should provide specific reasons which are based on their specific situation for why they object.

12.5. We cannot comply with the objection if we have compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual or if the processing is for the establishment, exercise or defence of legal claims.

12.6. In the instance that we cannot comply, we will clearly document our decision for this, inform the individual, inform them of their right to go to the ICO, or to seek judicial recourse.

13. Withdrawal of consent procedures

13.1. All people have the right to withdraw their consent to have their personal information shared at any time.

13.2. We guarantee that it will be as easy to withdraw consent as it is to give consent.

13.3. If an individual withdraws their consent to share information we will discuss in full and explain how this decision may impact on their health and care outcomes.

13.4. In certain instances, where legislation or public good outweighs the individual's right to not consent to information sharing, we may not be able to honour any withdrawal of consent. This will be discussed in detail and will only occur if we can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual.

13.5. Any time in which consent is not given or is withdrawn the Data Protection Champion will keep a log of this and a note will be made on the individual's records.

14. Responsibilities

14.1. The Data Protection Champion is responsible for maintaining records around Subject Access, Rectification, Erasure and Withdrawal of Consent requests.

14.2. The Data Protection Champion is also responsible for maintaining staff training on record keeping and auditing staff knowledge annually.

14.3. The Data Protection Champion will report to the DPO/Senior Management any Subject Access Requests or similar.

14.4. The Data Protection Officer has final say on any Subject Access decisions.

14.5. The Data Protection Champion will monitor compliance with the Record Keeping Policy and has responsibility for reviewing the policy at least annually.

15. Approval

15.1. This policy has been approved by the undersigned and will be reviewed at least annually.

Signed: 

Name: Kyle Jameson

Date: 09.08.2021

Date of next review: 09.08.2022