Customer DATA PROTECTION POLICY (including Data Retention)

Introduction

During your time with our Company (I Can Do That! CIC) you are likely to give us your personal information for example name, date of birth and home address. The UK's data protection legislation, including the General Data Protection Regulations (GDPR) contains strict principles and legal conditions which must be followed before and during any processing of any personal information.

The purpose of this policy is to ensure that you are aware of the reasons we are requesting your data, what data we can and cannot request and how it will be used and stored.

Definitions

Data Subject: a living individual.

Data Controller: the person or organisation that determines the means and the purpose of processing the personal data.

Data Protection Legislation: includes (i) the Data Protection Act 1998, until the effective date of its repeal (ii) the General Data Protection Regulation ((EU) 2016/679) **(GDPR)** and any national implementing laws, regulations and secondary legislation, for so long as the GDPR is effective in the UK, and (iii) any successor and supplemental legislation to the Data Protection Act 1998 and the GDPR, in particular the Data Protection Bill 2017-2019 and the E-Privacy Directive (and its proposed replacement), once it becomes law.

Personal data: is any information that identifies a living individual (data subject) either directly or indirectly. This also includes special categories of personal data. Personal data does not include data which is entirely anonymous or the identity has been permanently removed making it impossible to link back to the data subject.

Processing: is any activity relating to personal data which can include collecting, recording, storing, amending, disclosing, transferring, retrieving, using or destruction.

Special categories of personal data: this includes any personal data which reveals a data subject's, ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, genetic, biometric or health data, sex life and sexual orientation.

Criminal records data: means information about an individual's criminal convictions and offences, and information relating to criminal allegations and proceedings.

What are the GDPR principles?

We are a data controller. This means that we are required by law to ensure that everyone who processes personal data and special categories of personal data during the course of their work with us does so in accordance with the data protection legislation, including the GDPR principles. In brief, the principles say that:

- Personal data must be processed in a lawful, fair and transparent way.
- The purpose for which the personal information is collected must be specific, explicit and legitimate.
- The collected personal data must be adequate and relevant to meet the identified purpose.
- The information must be accurate and kept up to date.
- The personal data should not be kept in a form which permits identification of a data subject for longer than is necessary for the purposes for which it is used.

- The personal data must be kept confidential and secure and only processed by authorised personnel.

Other rules under the GDPR state that:

- The transfer of personal data to a country or organisation outside the EEA should only take place if appropriate measures are in place to protect the security of that data.
- The data subject must be permitted to exercise their rights in relation to their personal data.

The Company and all employees must comply with these principles and rules at all times in their information-handling practices. We are committed to ensuring that these principles and rules are followed, as we take the security and protection of data very seriously.

You must inform us immediately if you become aware that any of these principles or rules have been breached or are likely to be breached.

What are the lawful reasons under which we would expect you to process personal data?

Whilst carrying out our work activities we are likely to process personal data. The Company will only process personal data where the business has a lawful basis (or bases) to process that information. The lawful basis may be any one of the following reasons or a combination of:

a) Consent has been obtained the data subject to process their personal data for specified purposes.
b) Where we need to perform the contract we have entered into with the data subject either for employment or commercial purposes.
c) Where we need to comply with a legal obligation.
d) Where it is necessary for our legitimate interests (or those of a third party) and the interests and fundamental rights of the data subject do not override those interests.

There are other rare occasions where we may need to process the data subjects personal information, these include:

e) Where we need to protect the data subject's interests (or someone else's interests).
f) Where it is needed in the public interest [or for official purposes].

You will always be informed of which service you are being offered by the company and what data we need to help you on that service. You will also be informed of how we store and dispose of that data.

Privacy Notices

- Personal data must be processed in a lawful, fair and transparent way.

Before we begin to collect your data you will be advised of your privacy notice with us. The content of the privacy notice must provide accurate, transparent and unambiguous details of the lawful and fair reason for why we are processing the data. It must also explain how, when and for how long we propose to process the data subjects personal information. We need to include information around the data subjects' rights and most importantly, the notice should also explain how we will keep the information secure and protected against unauthorised use.

Where we intend to collect data indirectly from a third party or a public source (i.e. Jobcentre Plus), we must ensure that a privacy notice is issued to the data subject within a reasonable of period of obtaining the personal data and no later than one month; if the data is used to communicate with the individual, at the latest, when the first communication takes place; or if disclosure to someone else is envisaged, at the latest, when the data is disclosed.

We must only use data collected indirectly if you have evidence that it has been collected in accordance with the GDPR principles.

Purpose Limitation

- The purpose for which the personal information is collected must be specific, explicit and legitimate.

When we collect personal information we will set out in the privacy notice how that information will be used. If it becomes necessary to use that information for a reason other than the reason which we have previously identified we must usually stop processing that information. However, in limited circumstances we can continue to process the information provided that the new reason for processing the personal information remains compatible with our original lawful purpose (unless our original lawful basis was consent).

Adequate and relevant

- The collected personal data must be adequate and relevant to meet the identified purpose.

We must only process personal data where we have been authorised to do so because it relates to our work or we have been delegated temporary responsibility to process the information. We must not collect, store or use unnecessary personal data and must ensure that personal data is deleted, erased or removed within the Company's retention guidelines. We must not process or use personal data for non-work related purposes.

The Company will review its records on a regular basis to ensure they do not contain a backlog of out-of-date or irrelevant information and to check there are lawful reasons requiring information to continue to be held.

Accurate and kept up to date

- The information must be accurate and kept up to date.

If your personal information changes while benefiting from one of our services please inform your mentor as soon as possible so that the Company's records can be updated. The Company will not be responsible for any inaccurate personal data held on its systems where you have failed to notify it of the relevant change in circumstances.

Kept for longer than is necessary (Retention od Data)

- The personal data should not be kept in a form which permits identification of a data subject for longer than is necessary for the purposes for which it is used.

Different categories of personal data will be retained for different periods of time, depending on legal, operational and financial requirements.

I Can Do That! CIC operates various different projects and contracts, each of which has its own length

of time required to store the data relating to that contract/project.
Data will be stored in accordance with the individual contracts held unless not stated. In the case where a length of data retention is not specified, we will store data for 7 years and then confidentially shred all hard copies. Electronic copies will be stored for 10 years then deleted.

Kept confidential and secure

- The personal data must be kept confidential and secure and only processed by authorised personnel.

To achieve this we must follow these steps:

- The Company has in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to data. These procedures must always be adhered to and not overridden or ignored.
- Where the Company provides staff with code words or passwords to be used before releasing personal information, for example by telephone, staff must strictly follow the Company's requirements in this regard.
- Only transmit personal information between locations by fax or e-mail if a secure network is in place, for example, a confidential fax machine or encryption is used for e-mail.
- Ensure that any personal data which we hold is kept securely, either in a locked filing cabinet or, if it is computerised, it is password protected so that it is protected from unintended destruction or change and is not seen by unauthorised persons.
- Do not access another customers records without authority as this will be treated as gross misconduct and it is also a criminal offence.
- Do not write down (in electronic or hard copy form) opinions or facts concerning a data subject which would be inappropriate to share with that data subject.
- Do not remove personal information from the workplace with the intention of processing it elsewhere unless this is necessary to enable staff to carry out their job duties and has been authorised by their line manager.
- Staff must ensure that when working on personal information as part of their job duties when away from their workplace and with the authorisation of their line manager, they continue to observe the terms of this policy and the data protection legislation, in particular in matters of data security.
- Ensure that hard copy personal information is disposed of securely, for example cross-shredded.
- Manual personnel files and data subject files are confidential and are stored in locked filing cabinets. Only authorised employees have access to these files. For a list of authorised employees, please contact Amanda Moss 0791 505 3549 OR Lynda Wheeler 07897 310055. These will not be removed from their normal place of storage without good reason.
- Data stored on memory sticks, discs, portable hard drives or other removable storage media is kept in locked pedestals and not a normal storage solution for the company.
- Data held on computers are stored confidentially by means of password protection, inidivdual log ons and encryption. Personal customer data is NOT to be stored on laptop hard drives in case the laptop is stolen, this data must be stored in password protected systems used by I Can Do That!

CIC only.

- The Company has network back-up procedures to ensure that data on computers cannot be accidentally lost or destroyed. [More information on the Company's security policies can be obtained by contacting Amanda Moss 0791 505 3549].

Transfer to another country

- Transfer of personal data to countries or organisations outside of the EEA should only take place if appropriate measures are in place to protect the security of that data.

We do not generally have a need to transfer data outside of the European Economic Area (EEA). However, if we are requested to transfer personal data to a country or organisation outside of the EEA we must not transfer personal data to a country or organisation unless that country or organisation ensures an adequate level of protection in relation to the processing of personal data and have in place safeguards to ensure this is done. Staff must speak to [the Data Protection Officer – Amanda Moss] OR [Data Representative – Lynda Wheeler] before they send personal data outside of the EEA.

The data subject rights

- The data subject must be permitted to exercise their rights in relation to their personal data.

Under the GDPR, subject to certain legal limitations, data subjects have available a number of legal rights regarding how their personal data is processed. At any time a data subject can request that the Company should take any of the following actions, subject to certain legal limitations, with regard to their personal data:

- Allow access to the personal data
- Request corrections to be made to data
- Request erasure of data
- Object to the processing of data
- Request that processing restrictions be put in place
- Request a transfer of personal data
- Object to automated decision making
- Right to be notified of a data security breach

There are different rules and timeframes that apply to each of these rights. Staff must follow the Company's policies and procedures whenever they process or receive a request in relation to any of the above rights.

How should we respond to a data subject request?

Staff must follow the Company's data subject access procedure which details how to deal with requests and it describes the circumstances where a fee may be charged. The procedure includes the following:

- Always verify the identity of the person making a data subject request and the legitimacy of the request.

- A Data Access Request form should be issued for the Data Subject to complete, staff should forward this to [the Data Protection Officer – Amanda Moss] OR contact [Lynda Wheeler, our Data Representative].

- Staff are not to share personal information with a third party, unless the data subject has given their explicit prior consent to the sharing of their information. A third party is anyone who is not

the actual data subject and can include a family member of the data subject.

- We take great care not to accidentally share information with an unauthorised third party.

Be aware that those seeking information sometimes use deception in order to gain access to it so we will require ID as part of your data request.

Action to be taken in the event of a data protection breach

A personal data breach will arise whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on a data subject.

In the event of a security incident or breach, we must follow the Company's Data Breach Policy which includes immediately informing [the Data Protection Officer – Amanda Moss] OR [the Data Representative – Lynda Wheeler] so that steps can be taken to:

- Contain the breach;
- Assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen; and
- To limit the scope of the breach by taking steps to mitigate the effects of the breach.

The [Data Protection Officer – Amanda Moss] OR [Data Representative – Lynda Wheeler] will determine within 72 hours the seriousness of the breach and if the Information Commissioner's Office (ICO) and/or data subjects need to be notified of the breach.

Record keeping

- As we have fewer than 250 employees, we only need to document processing activities that:
    - are not occasional; or
    - could result in a risk to the rights and freedoms of individuals; or
    - involve the processing of special categories of data or criminal conviction and offence data.

Training

All employees that handle personal information of individuals must have a basic understanding of the data protection legislation, including the GDPR. Staff with duties such as computer and internet security, marketing and database management may need specialist training to make them aware of particular data protection requirements in their work area.

We provide staff with continuous training and updates on how to process personal data in a secure and confidential manner and in accordance with the spirit of the data protection legislation, including the GDPR. Staff are required to attend all training and to keep themselves informed and aware of any changes made to privacy notices, consent procedures and any other policies and procedures associated with our internal processing of personal data.

We must regularly review all our data processing activities and ensure that we are acting in accordance with the most current best practice and legal obligations in relation to data security and confidentiality.

Sharing personal data

We may share personal data internally as is necessary. We must always ensure that personal data is only shared with authorised persons and is shared in accordance with the purposes stated in any privacy notice or consents. Extra care and security must be taken when sharing special categories of data or transferring data outside of the Company to a third party.

Direct Marketing

We are subject to specific rules under the GDPR in relation to marketing our services. Data subjects have the right to reject direct marketing and we must ensure that data subjects are given this option at first point of contact. When a data subject exercises their right to reject marketing we must desist immediately from sending further communications.
However, as a company, we do not use direct marketing and we ill not use your data for such purposes.

Complaints

If you believe that this policy has been breached or to exercise all relevant rights, queries or complaints please in the first instance contact our DPO – Amanda Moss or DPR Lynda Wheeler on 0791 505 3549/07897 310055. You have the right to complain directly to the ICO (Information Commissioners Office) without contacting I Can Do That! CIC about any data security concerns.

Changes to this policy

We reserve the right to change this policy at any time so please always check this document regularly to ensure you are following the correct procedures.

This policy was last reviewed on 01.09.2025 and will be reviewed again on 01.09.2026