



GDPR and DATA PROTECTION POLICY

Version	Created by	Date Reviewed	Approved by	Next Review
1	Linda Wilcox	May 2024	Sue Fortune	June 2025

Table of Contents

<i>Purpose</i>	<i>2</i>
<i>Definitions.....</i>	<i>2</i>
<i>Principles</i>	<i>2</i>
<i>Safeguarding and Grant-Making to Organisations</i>	<i>3</i>
<i>Safeguarding and Grant-Making to Individuals.....</i>	<i>4</i>
<i>Other Lincs Links contact with children or adults at risk</i>	<i>4</i>
<i>Dealing with safeguarding concerns</i>	<i>4</i>
<i>Responsibility for implementing this policy.....</i>	<i>5</i>
<i>Breaches of the policy.....</i>	<i>6</i>

. DATA PROTECTION POLICY

1. PURPOSE OF THIS POLICY

We must comply with the GDPR.

This policy supports our information governance framework and defines data protection from The Company's perspective. It includes what the law requires in this respect, principally under the UK General Data Protection Regulation (**GDPR**), the UK law which replaced the EU General Data Protection Regulation.

The implementation of this Policy is overseen by the Data Protection Officer, to whom you should address all queries or concerns.

2. INTRODUCTION

We are committed to safeguarding personal information.

The Company obtains, keeps and uses personal information (also referred to as data) about our customers, job applicants and about current and former employees, temporary and agency workers, contractors, interns, supporters, stakeholders and apprentices for a number specific lawful purposes. This is set out in The Company's Privacy Statement, which all employees should be familiar with.

We are committed to complying with our data protection obligations, and to being concise, clear and transparent about how we obtain and use personal information, and how (and when) we delete that information once it is no longer required.

The Company is an organisation that processes personal information. Therefore, we are registered with the Information Commissioner on the Data Protection Public Register.

3. OVERSEEING OFFICER

The Company's data protection officer is responsible for informing and advising The Company and its staff on its data protection obligations, and for monitoring compliance with those obligations and with The Company's policies. If you have any questions or comments about the content of this policy or if you need further information, you should contact the data protection officer.

4. THE PRINCIPLES OF THE GDPR

You must adhere to the principles of the GDPR.

The Company will comply with the following data protection principles when processing personal information:

- we will process personal information lawfully, fairly and in a transparent manner;
- we will collect personal information for specified, explicit and legitimate

purposes only, and will not process it in a way that is incompatible with those legitimate purposes;

- we will only process the personal information that is adequate, relevant and necessary for the relevant purposes;
- we will keep accurate and up to date personal information, and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay;
- we will keep personal information for no longer than is necessary for the purposes for which the information is processed; and
- we will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

INFORMATION SECURITY

5. DATA PROTECTION IMPACT ASSESSMENTS (DPIA)

We will carry out risk assessments in accordance with the law.

Where processing is likely to result in a high risk to an individual's data protection rights (eg where The Company is planning to use a new form of technology or marketing strategy), we will, before commencing the processing, carry out a DPIA to assess:

- whether the processing is necessary and proportionate in relation to its purpose;
- the risks to individuals; and
- what measures can be put in place to address those risks and protect personal information.

Any DPIA should be overseen by the DPO.

6. WHAT IF A THIRD PARTY ASKS YOU TO SHARE INFORMATION?

Do not disclose personal information unless it is lawful to do so.

Sometimes we may be asked by a third party to share information about an individual or group of individuals e.g. the police or another organisation. Sometimes this is fine and sometimes it is not.

Staff should not worry about making these decisions. If everyone follows the procedures in place it will be clear when this is acceptable and when it is not. Our Privacy Statement details any information we may already know we intend to share and who with, so it may be clear from checking this if you should share the data being requested. However, if this is not clear and you are not sure then you must seek approval before sharing the information being requested. Send requests to the DPO.

7. INFORMATION SECURITY MEASURES

You must comply with these rules.

The Company will use appropriate technical and organisational measures to keep personal information secure, and in particular to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage. In particular, we have implemented the following measures and rules:

- **Emails**

- do not forward internal emails to external sources (you may carefully cut and paste sections of an email if absolutely necessary)
- do not use the “blind copy” feature and be cautious about clicking “reply all”
- personal information may only be shared with third parties where there is a legal justification – check with the DPO first

- **Paper files**

- Paper files must not be removed from the office without permission of the Chief Community Caring Officer
- Paper files must be stored in lockable filing cabinets
- Confidential information or material containing personal data must be destroyed, if required we will use Horncastle Data Shredding.
- Desks must be clear of personal information at the end of each day – check before leaving the office

- **IT and Computers**

- Use password protection and encryption where available on Charity systems to maintain confidentiality
- Computers and other electronic devices must be password protected and those passwords must be changed on a regular basis. Passwords should not be written down or given to others
- Computers and other electronic devices should be locked when not in use to minimise the risk of accidental loss or disclosure
- Confidential information must not be copied onto floppy disk, removable hard drive, CD or DVD or memory stick / flash-drive etc. without the express permission of the Chief Community Caring Officer
- Staff should ensure they do not introduce viruses or malicious code on to Charity systems. Software should not be installed or downloaded from the internet without it first being virus checked.

- **Third Parties**

- Generally, we should not share information with third parties. When we must do so, there must be a legal justification or reason – check with the DPO
- Personal information may only be shared with contractors when they are approved by the DPO and any necessary data sharing agreements are in place
- All personal data should only be shared on a “need to know” basis
- Visitors must not be left in the office unattended
- Do not give visitors access to the office WIFI unless with the Chief Community Caring Officer’s permission.

8. STORAGE AND RETENTION

We must only retain personal information where it is lawful to do so.

The GDPR states that data should not be kept for longer than necessary for the purpose for which it is held. Therefore, there are no definitive rules for how long data

should be held. Each situation should be dealt with on its own merit, but retention records should be justified.

As a general rule, however, The Company will hold data, including personal and special categories of data (formally, 'sensitive data'), for the following minimum periods, which may be extended where circumstances means it is fair and lawful to do so:

Data Type	Indicative retention period
Customer Records	<i>6 years from point of last contact with customer</i>
Unsuccessful job applicant	6 months
Employee who has left	6 years
PAYE records and other employee finance details	7 years
Other financial data	6 years
Volunteer who has left	3 years
Potential customer enquiry	9 months
Personnel and training records	2 years
Contracts and terms and conditions of employment	6 years
Working time opt and compliance records	2 years
Annual leave records	2 years
Immigration checks	<i>2 years from date employee leaves</i>
Other accounting records	7 years

9. DATA BREACHES

Data breaches must be reported immediately and in any event within 72 hours.

A data breach may take many different forms, for example:

- loss or theft of data or equipment on which personal information is stored;
- unauthorised access to or use of personal information either by a member of staff or third party;
- loss of data resulting from an equipment or systems (including hardware and software) failure;
- human error, such as accidental deletion or alteration of data;
- unforeseen circumstances, such as a fire or flood;
- deliberate attacks on IT systems, such as hacking, viruses or phishing scams; and
- 'blagging' offences, where information is obtained by deceiving the organisation which holds it.

The Company will:

- make the required report of a data breach to the Information Commissioner's Office without undue delay and, where possible within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals; and
- notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

You must notify the DPO immediately if you become aware of a data breach, or potential data breach, even if there are no apparent consequences.

10. YOUR OBLIGATIONS

You must not misuse personal information, or disclose it without authority, or take it home with you

You will have access to the personal information of other members of staff, suppliers and clients or customers of The Company in the course of your employment or engagement. The Company expects you to help meet its data protection obligations to those individuals at all times.

In respect of personal information to which you have access, you must:

- only access the personal information that you have authority to access, and only for authorised purposes;
 - only allow other Charity staff to access personal information if they have appropriate authorisation;
 - do not write down (in electronic or hard copy form) opinions or facts concerning a data subject which it would be inappropriate to share with that data subject;
 - only allow individuals who are not Charity staff to access personal information if you have specific authority to do so from the DPO;

- keep personal information secure at all times;
- not remove personal information, or devices containing personal information (or which can be used to access it), from The Company's premises unless appropriate security measures are in place (such as pseudonymisation, encryption or password protection) to secure the information and the device; and
- not store personal information on local drives or on personal devices that are used for work purposes.
- You should contact the DPO if you are concerned or suspect that one of the following has taken place (or is taking place or likely to take place):
- processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information, without one of the special conditions being met;
- any data breach (defined below);
- access to personal information without the proper authorisation;
- personal information not kept or deleted securely;
- removal of personal information, or devices containing personal information (or which can be used to access it), from The Company's premises without appropriate security measures being in place;
- any other breach of this policy or of any of the data protection principles (set out above).

11. OWN DEVICES

Do you not process Charity data on your own personal device(s) unless you have specific written permission from the Chief Community Caring Officer and the precautions below are observed at all times.

This means, for instance, that you should not access your work emails on a private phone or laptop, or take work home with you on a storage device and work on it through your home computer. It also means that you should never email work related documents to your personal email address.

Where you have permission to use your personal device for work, you must:

- Ensure that the device is kept safe and secure at all times and passcode protected;
- Ensure that you know how to, and are able to, erase data remotely in case of loss or theft;
- Ensure that your location settings (if applicable) are switched on and that, with phones and tablets, the Find My Phone or equivalent feature is enabled;
- Ensure that backups of any data are made to the Cloud.