Title of policy: Data Protection Policy

Unique ref number: CEOP01

Directorate: Office of the CEO

Department: Data Protection

Table of Contents:

Please note: this document contains links to other documents

1. Purpose:

1.1 This Data Protection Policy (“Policy”) together with the documents and other policies referred to within it regulates and details the way in which Guide Dogs (“GDBA”) obtains, uses, holds, transfers and processes Personal Data and Special Category Data about individuals and ensures that all employees know the rules for protecting Personal Data.

1.2 This Policy also describes individuals' rights in relation to their Personal Data processed by GDBA.

1.3 GDBA has practices in place in relation to their handling of Personal Data to ensure that they are acting in accordance with UK laws and other relevant regulatory guidance. The most notable legislation in this area is the Data Protection Act 1998 (DPA) and the General Data Protection Regulation (GDPR) due to be enacted in May 2018.

2. To whom the policy applies

2.1 All employees, workers and contractors are required to comply with the provisions of this Policy.

3. Main Principles:

3.1 General Principles:

GDBA shall comply with the principles of the GDPR to ensure that all data is:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to the data subject and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told the data subject about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told the data subject about.
- Kept securely
- At all times, GDBA will ensure that it has a legal basis for the processing of personal information.

GDBA is registered as a Data Controller with the Information Commissioner's Office (ICO). Our registration number is Z5672321. Phillippa Caine is the Data Protection Officer and is available to contact on any Data Protection issue by emailing: dataprotectionofficer@guidedogs.org.uk

3.2 Personal Data

"Personal Data" is any information (for example, a person's name) or combination of information about a living person (such as name and address and date of birth) which allows that living person to be identified from that information and which relates to them, such as the job application of "Joe Green" with his address and date of birth, or the appraisal record of "Sam Brown" with similar details. If in doubt, individual details should be treated as Personal Data.

Personal Data which may be used by GDBA in its day to day business relate to employees, volunteers, beneficiaries, supporters, job applicants, temporary staff, individual consultants or contractors, visitors etc.

Personal Data may also be relevant to unincorporated suppliers (such as a sole trader business or partnership), or inquirers or complainants. The definition of Personal Data also includes opinions about a person, and appraisals about or statements of intent regarding them.

The laws governing how GDBA can use Personal Data apply whether the Personal Data is stored electronically (for example, in emails, on IT systems, as part of a database or in a word-processed document) or in structured paper records (for example, in paper files, card indexes or filing cabinets or in a pile of papers that are intended to be filed or stored electronically).

3.3 Processing of Personal Data & Audits

GDBA uses or processes Personal Data (including Special Category Data,) on a range of individuals for a multitude of business purposes. Such individuals may include staff and contractors, volunteers, beneficiaries, supporters, business contacts, customers and prospects, job applicants and former employees, and the person whose Personal Data is used by GDBA is known as "the data subject".

When GDBA collects, stores, uses, discloses, updates or deletes or destroys Personal Data, this is called "processing". All processing is regulated by data protection legislation and must meet certain conditions to be carried out lawfully

GDBA holds a record of categories of personal data held across each functional area, has clear retention schedules and the Data Protection Officer (or their delegated representative) will keep this under regular review.

Personal Data and Special Category Data are held securely by GDBA and staff are regularly briefed on appropriate and safe data management.

3.4 Transparency and Personal Data

GDBA is entrusted to use the Personal Data of individuals on the basis that the proposed use is transparent, expected and clearly defined. Accordingly, one of the main data protection obligations requires GDBA to process Personal Data fairly.

In addition, use of Personal Data must be lawful. In practice, this means that GDBA will comply with at least one of the following conditions when processing Personal Data:

- the individual to whom the Personal Data relates has consented to the processing;
- the processing is necessary for the performance of a contract between GDBA and the individual (or to enter into that contract at the individual's request);
- the processing is necessary to comply with a legal obligation (not a contractual obligation) placed on GDBA;
- the processing is necessary to protect a vital interest of the individual (where there is an imminent risk to their life or of serious harm to them otherwise); or
- the processing is necessary to pursue the legitimate interest of GDBA (or a proposed recipient of the Personal Data) but where on balance, this would not involve disproportionate harm to the individual.

Use of Personal Data should meet one or more of these conditions. If there are any concerns about this; it is proposed to use Personal Data for additional purposes; or new reasons for using Personal Data are contemplated, reliance on these conditions must be discussed in the first instance with the Data Protection Officer prior to being relied upon.

All new Personal Data processing activities and projects involving the use of Personal Data must be approved prior to being started as there are complex exemptions and other lawful reasons for processing which may apply.

In addition, GDBA ensures its Personal Data is accurate and up to date. GDBA takes care to record and input Personal Data accurately. Some Personal Data may change from time to time (such as addresses and contact details, bank accounts and the place of employment). It is important to keep current records up to date. GDBA takes care to update records promptly and correctly.

3.5 Privacy Notices

When an individual gives GDBA any Personal Data about him or herself, GDBA will make sure the individual knows:

- for what purposes GDBA will process the Personal Data provided to it;
- sufficient details about any proposed disclosures/transfers of their Personal Data to Third Parties (including any cross-border transfers);
- the rights that the individual has in respect of their personal data;
- any other information that the individual should receive to ensure the processing carried out is within his/her reasonable expectations (retention periods for instance); and
- who to contact to discuss or raise any Personal Data issue.

GDBA does this by providing this information in what is known as a "privacy notice" or fair processing notice. Before collecting Personal Data, GDBA will give individuals providing those details appropriate Privacy Notices, these may be embedded in contracts, or on websites or form part of application or other forms. GDBA will inform individuals about the processing of their Personal Data before or at the time the data is collected. The information contained in its Privacy Notices will be concise and easily accessible and written in clear and plain language.

GDBA will only process Personal Data in a manner and for purposes consistent with the relevant privacy notice(s) already provided to an individual. Personal Data should not be collected for one purpose and then used for a second purpose unless that is also set out in the relevant notice.

3.6 Special Categories of Personal Data

Special Categories of Personal Data is data about a person's race or ethnicity, their health, their sexual preference, their medical information, genetic or biometric data, an individual's religious beliefs, their political views, trade union membership or information accusing an individual of any crime, or about any criminal prosecution against them, and the decision of the court and any punishment. The Data Protection Officer can provide further information on what is, and the handling of, Special Category Data in relation to our work.

Special Categories of Personal Data should not be collected or used unless essential. It must be treated as strictly confidential. Extra care must be taken with it and it must be kept more securely. In addition to the normal requirements for lawful use of any Personal Data such details should not be used without the explicit prior consent of the individual, which has to be clear,

unambiguous and voluntary.

GDBA does not seek to obtain Special Categories of Personal Data unless:

- It is to provide a service to a beneficiary;
- the individual concerned agrees in writing that we may do so on the basis of a full understanding of why GDBA is collecting the data
- GDBA needs to do so to meet its obligations or exercise its rights under any relevant laws; or
- in exceptional circumstances such as where the processing is necessary to protect the vital interests of the individual concerned

Please note that the “legitimate interest” criteria described above alone is not enough to process Special Categories of Personal Data.

Special Categories of Personal Data should not be disclosed unless measures are taken to encrypt or otherwise secure that information due to the potential for harm or distress if the email is received by unintended recipients or otherwise goes astray.

Special Categories of Personal Data should be collected and used as little as possible and be subject to more limited and strictly need to know access and used subject to greater security measures than other Personal Data.

Other Personal Data where misuse may lead to distress or harm, especially to fraud or identity theft (for example, bank account or credit card details, or official government identification numbers, such as national insurance contribution numbers) must be treated like Special Categories of Personal Data.

3.7 Staff Obligations

All GDBA staff should be aware of their obligations and comply at all times with this Policy.

All staff must ensure that Personal Data is processed in accordance with the principles of the GDPR (as summarised in GDPR Principles above) and the terms of this Policy.

All staff must familiarise themselves with the GDBA privacy policies including in relation to Candidates, Staff and Customers/Third Parties and ensure that any Personal Data they process is handled in accordance with those policies.

All staff involved must:

- Read and understand this policy
- Use complex passwords in accordance with the IS policy http://www.gdba.internal/Home/Directorates/BusinessandFinanceServices/InformationServices/PoliciesProcedures/tabid/904/Default.aspx
- Only keep information as long as necessary and comply with GDBA's Retention Policy
- Not download personal data onto personally owned devices and ensure that they comply with the IS and Acceptable Usage Policy
- Will comply with GDBA policies in relation to IT and Communications Systems and data security
- Be aware of the risks of transporting data and comply with GDBA policy in relation to data security and homeworking.
- Report any breaches of this policy immediately in accordance with GDBA Data Breach Procedure
- Notify the Data Protection Officer immediately and in accordance with GDBA Subject Access Request Procedure, if they are in receipt of a subject access request from anyone.
- Notify the Data Protection Officer immediately, if they receive a request from anyone in relation to the rights listed in clause 10 below.

3.8 Data Retention & GDBA Archives

Personal Data must be stored securely and not be kept for any longer than required. Some records have to be retained for minimum periods by law (such as records on employee payments and their taxation under tax laws).

As a general rule, when Personal Data is no longer needed for the purposes for which it was collected, this Personal Data will be securely and permanently destroyed as soon as practicable. GDPR Retention Policy sets out details of how long certain categories of data will be retained and the process for reviewing this.

GDBA will not delete or destroy or amend records containing Personal Data without explicit consent once they have been informed those records have been requested by the individual whose Personal Data it is, or by a Data Protection Authority. Such a breach may be a criminal offence with personal liability.

3.9 The Right to Information, the Right to Erasure and Subject Access Requests

Individuals have certain rights in relation to their Personal Data:

- the right to obtain information (what Personal Data, from where, used for what purposes and shared with which recipients) about Personal Data held about

themselves and to obtain copies of such Personal Data (Subject Access Request);
- the right to prevent processing of Personal Data for direct marketing purposes;
- the right to object to and stop certain processing of Personal Data where it is likely to cause substantial unwarranted harm or distress;
- the right to have Personal Data corrected;
- the right to compensation for any damage/distress suffered from any breach;
- the right to be informed of automated decision making about them.

If any member of GDBA staff receives such a request or demand from an individual, they must promptly inform the Data Protection Officer.

Individuals are also allowed to withdraw their consent to GDBA's use of their Personal Data at any time. If a GDBA employee receives such a withdrawal of consent, they must promptly inform the Data Protection Officer.

If anyone at GDBA receives a request to stop sending fundraising materials, direct marketing communications of that type to that individual must be stopped as soon as is possible.

Individuals can also ask in writing for copies of their Personal Data which GDBA holds about them and other details about how GDBA uses their Personal Data.

Subject to receipt of proof of ID where considered necessary, and following receipt of a written request from an individual for access to his/her Personal Data, GDBA will (to the extent requested by the individual) provide any information required in accordance with our Subject Access Request Procedure.

Strict rules must be followed as part of this process. Therefore, any such request received should be passed on to the Data Protection Officer for logging.

There is a right under data protection legislation known as "the right to be forgotten". This gives an individual the right to have their data erased when there is no compelling reason for continued processing. Under the DPA, the right to erasure is limited to processing that causes unwarranted and substantial damage or distress. Under the GDPR, this test is not present. However, if the processing does cause damage or distress, this is likely to make the case for erasure stronger.

3.10 Data Security

GDBA endeavours to keep all Personal Data secure by protecting data against being accessed by other companies or individuals (for example, via hacking), from being corrupted (data corruption) or being lost or stolen. This applies to Personal Data in IT systems, emails and attachments and paper files.

For example, staff (and GDBA Contractors where relevant) each have a password and individual controlled access rights to IT systems through their GDBA computer and/or mobile or other electronic device. For further information, please refer to the IT and Communication Systems policy in the Staff Handbook.

Staff must comply with our security procedures whenever processing Personal Data. GDBA is dependent on all employees to help keep Personal Data secure. Employees must only access and use Personal Data they are individually authorised to access and use, and which is needed for a specific task within their role.

Employees who work away from the charity's premises must comply with any additional procedures and guidelines issued by GDBA for home working and/or offsite working. Extra care is needed to secure Personal Data in such cases, particularly Special Category Data.

GDBA also recognises that adequate security is important where it arranges for Third Parties to process Personal Data on its behalf, such as when outsourcing services to service providers, who process Personal Data on behalf of GDBA as a result ("a Data Processor"). GDBA remains liable for those service providers and their treatment of the Personal Data. We will have suitable written contracts in place with such service providers with specific terms included to protect the Personal Data provided to them.

3.11 Disclosing Personal Data to Third Parties and Overseas Transfers

A disclosure of Personal Data is a form of processing. That means that the rules described above for fair and lawful use have to be satisfied. We will not disclose Personal Data to a Third Party without first checking the disclosure is lawful and proportionate.

There are some exceptions to deal with disclosures, such as those requested lawfully by Police where the information is necessary to prevent or detect a crime. Any request for Personal Data about an individual from government, Police or other similar bodies or from journalists or other investigators should be passed immediately to the Data Protection Officer.

From time to time GDBA may pass Personal Data (including special categories of personal data where appropriate) to third parties where lawful to do so; appropriate checks will be carried out on those third parties to ensure that data will be secure.

Unlawful disclosure (however well-meaning and however seemingly authoritative by the requestor) risks placing GDBA in breach of several obligations under data protection legislation. Special care is needed with

telephone requests for information, often used by unauthorised parties to 'blag' or obtain Personal Data to which they are not entitled. Employees must be certain of the identity of the person with whom they are dealing, ideally have a written request for information from them and ensure any disclosures are justified and authorised in advance.

There are special rules on whether Personal Data can be transferred to another country. Within the EU, there are restrictions on the transfer of Personal Data outside of the European Economic Area (EEA) (such a transfer can happen, for example, where Personal Data is emailed outside the EEA; where our IT servers are hosted outside the EEA; or where there is remote on-screen access from outside the EEA to Personal Data stored in an IT system within the EEA). This is to make sure the Personal Data remains safeguarded and that the individuals concerned do not lose the protection and rights they have under local law in respect of their Personal Data when transferred.

Actual or likely transfers of Personal Data to outside the EEA, especially of Special Categories of Personal Data, should be clearly set out in the privacy notices described in the fair use section of this Policy (section 5) above so that such transfers are expected by the affected individuals.

3.12 Fundraising

As with other types of Processing, the use of Personal Data for fundraising must satisfy the fair and lawful use requirements set out above. This means information notices must be given, and a lawful reason for processing must be satisfied.

Where there is a clear legitimate interest, which we can evidence, Legitimate Interest should be used as the justification for processing personal data. To do so it is necessary to balance our legitimate business interest with the rights of the individual.

Individuals have a right to decline postal marketing and to object to any marketing activity. Any objections to fundraising communications or requests to unsubscribe must be dealt with properly and promptly and individuals must be offered an easy way to unsubscribe.

4. Responsibilities:

- The Data Protection Officer of Guide Dogs oversees the administration of this policy.
- All staff, contractors and volunteers that have contact with Guide Dogs data have a responsibility to implement the Policy. Advice and guidance is available from the Data Protection Officer.

- Guide Dogs will provide training, supervision and line management.

5. Monitoring:

Legislation and Guidance that underpins the Data Breach Policy, Procedures and Processes:

- General Data Protection Regulation (GDPR)
- Data Protection Act 2018

6. Document Management

- Owner: Phillippa Caine
- Job Title: Data Protection Officer
- Author: Linda Jackson
- Job Title: GDPR Data Manager
- Approved Date: May 2018
- Last Reviewed Date: May 2018
- Review Frequency: Every two years
- Next Review Due: May 2020

7. Version control table:

Please note the table below contains 2 rows and 5 columns. Other rows may be added as required.

Version No.	Detail of change / sign off	Author / Name	Position	Date
1.0		Linda Jackson	GDPR Data Protection	18/05/2018

End of document