Camden Giving
Data Protection Policy

Policy prepared by: Danielle Green
Policy approved by board on: 26/06/2018
Policy became operational on: 26/06/2018
Next review date: 26/06/2021

Overview of policy

1.1 Camden Giving needs to gather and use certain information about individuals. These can include employees, board members, grant applicants, business contacts, and other people the organisation has a relationship with or may need to contact.

1.2 This policy sets out how we seek to protect personal data and ensure that staff understand the rules governing their use of personal data to which they have access in the course of their work. Camden Giving has a commitment to protecting the rights and freedoms of data subjects and safely and securely processing their data in accordance with all of our legal obligations.

1.3 This policy ensures Camden Giving:

- Complies with current data protection law, including General Data Protection Regulation
- Follows good practice and compliance relating to personal data and communication
- Protects the rights of staff, board members and other associated individuals of whom we process their personal data
- Is transparent and accountable for how and why we collect, store, process and retain an individual's personal data
- Protects itself from the risks of a data breaches, reputational damage, using personal data unlawfully and/or inappropriately, and other associated risks
- Informs employees of their individual responsibilities, obligations and duty of care

1.4 The purposes for which personal data may be used by us include personnel, administrative, financial, regulatory, payroll and business development purposes.

Camden Giving's purposes for processing personal data includes the following:

- Compliance with our organisational, legal, regulatory and governance obligations and good practice
- Gathering information as part of our organisational duties and responsibilities to enable us to operate effectively and purposefully
- Administrative purposes such as processing employee details, monitoring and managing staff access to systems and facilities and staff absences, monitoring staff conduct, disciplinary matters

- Operational reasons, such as recording information on grant applications and processing payments
- Marketing our organisation and in some cases those we are affiliated with
- Improving our services, impacts and strategy
- Investigating complaints and illegitimate activity

Our Roles and Responsibilities

2.1 This policy applies to all staff, trustees and volunteers at Camden Giving. Staff must be familiar with this policy and comply with its terms. We are a new organisation so may supplement or amend this policy by additional policies and guidelines from time to time, to keep us in line with current legislation. Any new or modified policy will be circulated to staff before being adopted.

2.2 Responsibilities:

Trustees are ultimately responsible for ensuring that Camden Giving meets its legal obligations.

Data Protection Officer (DPO) has overall responsibility for the day-to-day implementation of this policy. This includes:

- Keeping the board updated about data protection responsibilities, risks and issues.
- Reviewing all data protection procedures and related policies, in line with an agreed schedule
- Arranging data protection training and advice for the people covered by this policy.
- Handling data protection questions from staff and anyone else covered by this policy • Dealing with requests from individuals to see the data Camden Giving holds about them (also called 'subject access requests').
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

Employees managing/using IT Systems are responsible for:

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services the company is considering using to store or process data. For instance, Microsoft Office 365 One Drive and BT My Donate.

Employees managing/sending Marketing Communication are responsible for:

- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.

2.3 General staff guidelines

- The only people able to access data covered by this policy should be those who need it for their work.
- Data should not be shared informally. When access to confidential information is required, employees can request it from their line managers.
- Camden Giving will provide training to all employees to help them understand their responsibilities when handling data.
- Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
- In particular, strong passwords must be used, changes every 3 months and they should never be shared.
- Personal data should not be disclosed to unauthorised people, either within the company or externally, unless consent is given.
- Data should be regularly reviewed and updated if it is found to be out of date and no longer required it should be deleted and permanently disposed of. If the data is no longer required for it's original purpose but is needed to ensure we comply with safeguarding procedures, it should be archived or supressed.
- Employees should request help from their line manager or the data protection officer if they are unsure about any aspect of data protection.

2.4 Data storage guidelines

These rules describe how and where data should be safely stored. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:

- When not required, the paper or files should be kept in a locked drawer or filing cabinet.
- Employees should make sure paper and printouts are not left where unauthorised people could see them, like on a printer.
- Data printouts should be shredded and disposed of securely when no longer required. When data is stored electronically, it must be protected from unauthorised access, accidental deletion and malicious hacking attempts:
- Data should be protected by strong passwords that are changed regularly and never shared between employees.
- If data is stored on removable media (like a USB), these should be kept locked away securely when not being used.
- Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing service.
- Servers containing personal data should be sited in a secure location, away from general office space.
- Data should be backed up frequently. Those backups should be tested regularly, in line with the company's standard backup procedures.
- Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.

- All servers and computers containing data are protected by approved security software and a firewall

Principles and Procedures

3.1 The General Data Protection Regulation (GDPR) is a legal framework that sets guidelines for the collection and processing of personal information of individuals within the European Union (EU). The GDPR sets out the principles for data management and the rights of the individual, while also imposing fines that can be revenue based.

3.2 Camden Giving shall comply with the principles of data protection enumerated in all General Data Protection Regulations. As a new organisation, we will make every effort possible in everything we do to comply with these principles and seek guidance wherever possible to meet the legal requirements.

3.3 Accountability and Transparency

We must ensure accountability and transparency in all our use of personal data. We are responsible for keeping a written and updated record of all the data processing activities and we are responsible for complying with each of the principles. Camden Giving are responsible for understanding our particular responsibilities to ensure we meet the following data protection obligations:

- Maintain up to date and relevant documentation on all processing activities using the Information Asset Register (IAR)
- Conducting Data Protection Impact Assessments (DPIA)
- Implement measures to ensure privacy by design and default, including:
  Data minimisation, pseudonymisation, transparency, allowing individuals to monitor processing, creating and improving security and enhanced privacy procedures on an ongoing basis
- Assessing current practice and developing a data privacy governance structure which includes appointing a Data Protection Officer;
- Implementing appropriate Privacy Notices;
- Refreshing and obtaining appropriate consents;
- Using appropriate organisation and technical measures to ensure compliance with the data protection principles, including protection of data and processes for retention and deletion of data;
- Creating breach, complaints and disciplinary reporting mechanisms.

3.4 Fair and lawful processing

We must process personal data fairly and lawfully in accordance with individuals' rights under the first Principle. This generally means that we should not process personal data unless the individual whose

details we are processing has consented to this happening. If we cannot apply a lawful basis, our processing does not conform to the first principle and will be unlawful. Data subjects have the right to have any data unlawfully processed erased.

3.5 Lawful basis for processing data

We must establish a lawful basis for processing data. It is your responsibility to check the lawful basis for any data you are working with and ensure all of your actions comply the lawful basis. At least one of the following conditions must apply whenever we process personal data:

1. **Consent** We hold recent, clear, explicit, and defined consent for the individual's data to be processed for a specific purpose.
2. **Contract** The processing is necessary to fulfil or prepare a contract for the individual.
3. **Legal obligation** We have a legal obligation to process the data (excluding a contract).
4. **Vital interests** Processing the data is necessary to protect a person's life or in a medical situation.
5. **Public function** Processing necessary to carry out a public function, a task of public interest or the function has a clear basis in law.
6. **Legitimate interest** the processing is necessary for our legitimate interests. This condition does not apply if there is a good reason to protect the individual's personal data which overrides the legitimate interest.

Special categories of personal data

This is data about an individual which is more sensitive, so requires more protection. This type of data could create more significant risks to a person's fundamental rights and freedoms, for example by putting them at risk of unlawful discrimination. The special categories include information about an individual's:

- Race
- Ethnic origin
- Political preference
- Religion
- Genetics
- Biometrics (where used for ID purposes)
- Health
- Sexual orientation

In most cases where we process special categories of personal data we will require the data subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

The condition for processing special categories of personal data must comply with the law. If we do not have a lawful basis for processing special categories of data that processing activity must cease.

3.6 Controlling and processing data

Camden Giving is classified as a data controller and data processor and lawfully control and process data. As a data processor, we must:

- Not use a sub-processor without written authorisation of the data controller
- Co-operate fully with the ICO or other supervisory authority
- Ensure the security of the processing
- Keep accurate records of processing activities
- Notify the controller of any personal data breaches

As a data controller, we must only appoint processors who can provide sufficient guarantees under GDPR and that the rights of data subjects will be respected and protected.

As a data processor, we must only act on the documented instructions of a controller. We acknowledge our responsibilities as a data processor under GDPR and we will protect and respect the rights of data subjects.

Third Party Data Processors

Data processors are third parties who provide elements of our services for us. We must have contracts in place with our data processors which means that they cannot do anything with personal information unless we have instructed them to do it. They will not share personal information with any organisation apart from us. They will hold it securely and retain it for the period we instruct. More information on how Camden Giving use personal data are found in our separate Privacy Policies.

The data processors we use are listed below:

Data Processor	Whose data is being stored
CAF Bank	Employees and Successful Grantees
Beehive Accounts	Employees and Successful Grantees
EventBrite	General Public including Businesses, Individuals and Voluntary Organisations
MailChimp	General Public including Businesses, Individuals and Voluntary Organisations
GIFTS Online	All Grant applicants and Individuals we send comms to
Salesforce & Form Assembly	All Grant applicants and Individuals we send comms to
Virgin Money Giving, STRIPE, Benevity, Amazon Smile	General Public including Businesses (Employees) and Individuals
HMRC	Employees
NEST Pensions	Employees
360 Giving	Successful Grantees

Personal Data Records

4.1 Creation of records

The individual or department that authored, created or is the primary custodian of a record is responsible for ensuring it is retained and destroyed in accordance with this policy. All records and other communications pertaining to Camden Giving are to be appropriately and accurately worded. You must act responsibly, lawfully and professionally when creating records regarding our business activities and/or on our systems.

Camden Giving prohibits staff from creating records that are misleading, intentionally false, fraudulent, sexually explicit, abusive, offensive, harassing, discriminatory, profane, libelous, defamatory, unethical, or that violate any laws, regulations or internal policies.

4.2 Storing and Communication

The documentation outlined below details all aspects of how Camden Giving receives, stores, processes, uses and manages personal data. Camden Giving will review the following documentation annually to ensure that it is still relevant and complaint with GDPR. We will update the information as regularly as required. **4.3 Information Asset Register**

This is where we store information on personal data we hold, where it came from, who we share it with and how it's stored. It also identifies how long we retain asset information for and we will monitor this closely. We will complete data audits to manage and mitigate risks to inform the Information Asset Register.

4.4 Privacy Notices

This is where we outline how we use different personal data. A privacy notice must be supplied at the time the data is obtained if obtained directly from the data subject. If the data is being used to communicate with the individual, then the privacy notice must be supplied at the latest when the first communication takes place. Users of our services including website, grant applications, fundraising will be stored on our website and email footers. Information relating to employees, trustees and volunteers is circulated internally and can be found on our shared One Drive account. .

4.5 Data Protection Impact Assessment

This is how we identify, assess and record data protection, information security and privacy risks and provide detailed information on how we mitigate the risks according to the risk level.

4.6 CRM Database

We will manage our communication consent and preferences of individuals whose data we store using *Gifts Online*. We will keep records demonstrating that our supporters have actively opted in to receive communication and we will also store communication preferences and be able to associate those preferences with the communication through which the supporter actively opted-in. We will manage changes in preferences when requested by supporters by running monthly reports from our email marketing software (Mailchimp) listing who has unsubscribed and we allow subscribers to

'unsubscribe' or 'manage preferences'. We will make a note in their file to when their data should be refreshed consent or deleted.

Retention of information

5.1 We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

5.2 Information relation to retention periods for each type of data asset we store and the method for deleting/destroying the data can be found in the Information Asset Register. We periodically review and update the document with additional record types. The Data Protection Officer will be responsible for monitoring the retention and disposal of data

5.3 Our records should not be disposed of or destroyed before the relevant retention period expires. Where more than one retention period applies to a record, it should be retained in accordance with the longest retention period, unless otherwise directed by the Data Protection Officer. If a record type is not listed in the Information Asset Register, contact the Data Protection Officer for guidance.

5.4 All records that hold personal information must be destroyed at the end of the relevant retention period, unless the retention period has been suspended. Any electronic data that is deleted is also purged to ensure that it is permanently removed from the servers.

5.5 On occasion, it may be necessary to retain some records for longer than the stated retention period, eg confirmation of attendees for a fundraising event booked several months in advance. However, once the record is no longer needed, it should be destroyed promptly.

Individual Rights

6.1 Subject Access Requests

Any individual including employees whose data we store (electronically or physically) have the right to ask for a copy of the information we hold about them via a 'Subject Access Request'. For employees, this includes information about grievance and disciplinary issues. We will respond to their request within 40 days from the subject access request.

6.2 Any request for personal information we may hold the should be in writing and addressed to admin@camdengiving.org.uk or Camden Collective, 5-7 Buck Street, London, NW1 8NJ. We will try to deal with requests informally, for example by providing the specific information required over the telephone, within 40 days from receiving the request. If we do hold information about the individual requesting information, they can ask us to correct any mistakes by contacting us as stated above.

6.3 If we do hold information about the data subject we will:

- give them a description of it;
- tell them the purposes for processing the information, why we are holding it and where we got it from;
- tell them who it could be disclosed to; and
- let them have a copy of the information in an intelligible form.

6.4 Any request for personal information we may hold the should be in writing and addressed to admin@camdengiving.org.uk or Camden Collective, 5-7 Buck Street, London, NW1 8NJ. We will try to deal with requests informally, for example by providing the specific information required over the telephone, within 40 days from receiving the request. If we do hold information about the individual requesting information, they can ask us to correct any mistakes by contacting us as stated above.

6.5 We may be entitled to withhold information if the information you have asked for contains information that relates to another person. Unless the other person gives their permission, or it is reasonable in all the circumstances to provide the information without permission, we are entitled to withhold this information.

6.6 Changes to preferences and consent

We will only communicate with individuals based on their consent to the collection and use of their information in accordance with the purposes they have requested, and in line with the retention schedules. Data subjects have a choice about whether they want to receive communication from Camden Giving that is of legitimate interest and/or benefit to them. They can change marketing and communication preferences at any time by contacting us by post to Camden Collective, 5-7 Buck Street, London, NW1 8NJor by email to admin@camdengiving.org.uk, or through MailChimp (for direct marketing only).

6.7 Rights to erasure

Individuals have a right to have their data erased and for processing to cease in the following circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected and / or processed
- Where consent is withdrawn
- Where the individual objects to processing and there is no overriding legitimate interest for continuing the processing
- The personal data was unlawfully processed or otherwise breached data protection laws
- To comply with a legal obligation
- The processing relates to a child

Data Breaches

7.1 Any breach of this policy or of data protection laws must be reported as soon as practically possible. Camden Giving has a legal obligation to report any data breaches to the ICO within 72 hours after being aware of the breach (unless there is a low risk to the individual's rights).

7.2 All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the [name of supervisory authority] of any compliance failures that are material either in their own right or as part of a pattern of failures

7.3 Any member of staff who fails to notify of a breach, or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

7.4 Please refer to our Data Breach reporting form to log the details of the breach.

Complaints

8.1 Camden Giving tries to meet the highest standards when collecting and using personal information. For this reason, we take any complaints we receive about this very seriously. When we receive a complaint from a person we make up a file containing the details of the complaint. This normally contains the identity of the complainant and any other individuals involved in the complaint. We will only use the personal information we collect to process the complaint and to check on the level of service we provide.

8.2 We usually have to disclose the complainant's identity to whoever the complaint is about. This is inevitable where, for example, the accuracy of a person's record is in dispute. If a complainant doesn't want information identifying him or her to be disclosed, we will try to respect that. However, it may not be possible to handle a complaint on an anonymous basis.

8.3 We will keep personal information contained in complaint files in line with our retention procedures. It will be retained in a secure environment and access to it will be restricted according to the 'need to know' principle.

8.4 Where enquiries are submitted to us we will only use the information supplied to us to deal with the enquiry and any subsequent issues and to check on the level of service we provide.
8.5 Please refer to our Complaints Reporting form to log any details of complaints.

Training

9.1 You will receive adequate training on provisions of data protection law specific for your role. You must complete all training as requested.

9.2 If you move role or responsibilities, you are responsible for requesting new data protection training relevant to your new role or responsibilities.

9.3 If you require additional training on data protection matters, contact the Data Protection Officer.

Failure to Comply

10.1 Camden Giving takes compliance with this policy very seriously. Failure to comply puts staff, Camden Giving and the data subjects at risk. It also carries the risk of significant civil and criminal sanctions for the employee and Camden Giving, and may, in some circumstances, amount to a criminal offence by the individual.

10.2 The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures, and this action may result in dismissal for gross misconduct. If a non-employee breaches this policy, they may have their contract terminated with immediate effect.

10.3 The Data Protection Officer has overall responsibility for this policy. They will monitor compliance with this policy regularly to make sure it is being adhered to.

10.4 Staff with any questions or concerns about anything in this policy should not hesitate to contact the Data Protection Officer.