Data Protection Policy

Active Date:	25th May 2018, revised 1st March 2022
Status:	Live
Review Date:	Annually
Revision history:	Version 1: 25th May 2018 Version 2: 1st March 2022 Key changes include: • New brand and contents page • Changes in staff • Updates to reflect planned CRM developments • Adding elements to formalise Cyber Essentials requirements • Brexit changes and compliance updates • Revisions to language to increase accessibility

1. Introduction

This Policy sets out the obligations of 360 Giving, a company registered in England under number 09668396, whose registered office is at **5th floor, 90 York Way, London, N1 9AG** ("360Giving") regarding data protection and the rights of staff, directors, contractors, volunteers, professional contacts and members of the public ("data subjects") in respect of their personal data under the Data Protection Act 2018 (UK General Data Protection Regulation ("GDPR") and the Privacy and Electronic Communications Regulations 2003 ("PECR").

This Policy sets 360Giving's obligations regarding the collection, processing, transfer, storage, and disposal of personal data. The procedures and principles set out herein must be followed at all times by 360Giving, its employees, agents, contractors, or other parties working on behalf of 360Giving.

360Giving is committed not only to the letter of the law, but also to the spirit of the law and places high importance on the correct, lawful, and fair handling of all personal data, respecting the legal rights, privacy, and trust of all individuals with whom it deals.

1.1 Definitions

Personal data

Any information relating to an identified or identifiable natural person, also known as a 'Data Subject' under GDPR, who can be identified, directly or indirectly, for example by name, an identification number, online identifiers, or any other data. 360Giving collects, stores and processes data relating to employees, trustees, event participants, publishers, funders, donors, consultants etc. All data collected about individuals is personal data under the GDPR.

In order to carry out its business and monitor the positive impact of 360Giving, we collect both personal and special category data.

Special categories of personal data

Under the GDPR special categories of personal data includes data relating to:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade-union membership
- The processing of genetic data and biometric data for the purpose of uniquely Identifying a natural person
- Health data
- Data about natural person's sex life or sexual orientation

360Giving commits to minimise the data that is collected, collect it anonymously and report in aggregate wherever possible, and ensure that special measures are put in place to protect the data and minimise any associated risks posed as a result of processing this data.

Data Controller

Under the GDPR, 360Giving is referred to as the 'Data Controller' (i.e. the party responsible for personal data, collected, used and processed) and is responsible for determining the purposes for collecting the data and ensuring effective data management practice to carry out its business and maintaining compliance with the GDPR.

Data Processor

Under the GDPR, the Data Processor is any person, third party or organisation that processes personal data on behalf of a Data Controller (i.e. 360Giving). For example, third party software suppliers (e.g. Salesforce, MailChimp) are the Data Processor on behalf of 360Giving.

Data Subject

Under the GDPR the Data Subject is any living individual (i.e. staff, trustees, training participants etc) whose personal data 360Giving collects, stores and processes.

Legitimate Interest

This is one of the bases for processing data under GDPR. Theoretically, it applies whenever an organisation uses personal data in a way that the data subject would expect. 'Interests' can refer to almost anything here, including an organisation or third party's commercial interests or wider societal benefits.

In general, the condition applies when:

- The processing isn't required by law, but there's a clear benefit to it;
- There is little risk of the processing infringing on data subjects' privacy; and
- The data subject should reasonably expect their data to be used in that way.

An example might include processing for payroll calculations and payments.

Processing

Under the GDPR, 'processing' means any operation or set of operations which is performed on personal data or sets of personal data. The processing can be automated or non-automated means and includes:

- Collection
- Recording
- Organisation/structuring
- Storage
- Adaptation/alteration
- Retrieval/access to
- Transmission/dissemination (e.g. sharing with other parties or transferring to another location)
- Erasure or destruction

Profiling

Under the GDPR 'profiling' refers to an activity that is carried out by automated/non-automated means to evaluate certain aspects of an individual's behaviour, preferences etc. For example, if 360Giving wished to profile job applicants by allocating a geo-demographic code to individuals, this would be classed as profiling. Under the GDPR, individuals have the right to object to profiling and have a right to be informed about the existence of profiling, of measures based on that profiling and the envisaged effects of profiling on the individual (e.g. selection for jobs or increased communications etc).

Personal data breach

Under the GDPR a personal data breach is an event that leads to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. Under the GDPR 360Giving has an obligation to report personal data breaches to the Information Commissioners Office (ICO), and in some cases, the Charity Commission. Where the breach is likely to adversely affect the individuals (i.e. Data Subject(s)) they should also be informed. Further information can be found in the Data Breach section below.

Consent

Under the GDPR, consent should be freely given (e.g. by a statement or clear affirmative action) of the Data Subject's agreement to processing their personal data. When capturing consent, the

wording used by 360Giving should be specific and unambiguous, meaning that the Data Subject is informed of what they are consenting to in order for 360Giving to process their personal data.

Third party

Under the GDPR a third party is a natural or legal person, public authority, agency or body that is not the Data Controller or Data Processor. For example, in order for a venue to host a training event, they might require attendee data for registration purpose and to satisfy their internal security checks.

Filing system

Under the GDPR a filing system refers to any physical or electronic system that stores personal data which is accessible to users according to specific criteria (e.g. alphabetical etc).

2. The Data Protection Principles

This Policy aims to ensure compliance with the GDPR. The GDPR sets out the following principles with which any party handling personal data must comply. All personal data must be:

2.1 Principle 1: Processed lawfully, fairly, and in a transparent manner in relation to the data subject.

360Giving is committed to communicating at the point of collecting data, and through its privacy notice in a clear and intelligible way using clear and plain language. 360Giving commits to using clear and plain language and ensuring that all individuals, particularly whose data we collect fully understand why we are collecting their data, what they are consenting to, and whether there are potential consequences of supplying that data.

2.2 Principle 2: Collected for specified, explicit, and legitimate purposes.

360Giving commits to obtaining personal data for specified purposes and will not use the personal data for a purpose that differs from those formally notified to the Data Subject(s) and notified to the ICO as part of 360Giving's GDPR register of processing. 360Giving's Privacy Procedure sets out the relevant procedures.

2.3 Principle 3: Adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

360Giving's Data Protection Lead is responsible for ensuring that 360Giving does not collect information that is not strictly necessary for the purpose for which it is obtained as outlined in its Data Asset Register. 360Giving will ensure that:

- All data collection forms (electronic or paper-based) must include a fair processing statement and link to 360Giving's Privacy Statement which must be approved by the Data Protection Lead

- 360Giving's Data Protection Lead will ensure that all data collection methods are reviewed on an annual basis to ensure that collected data continues to be adequate, relevant and not excessive in line with 360Giving's Data Protection Impact Assessment Procedure

2.4 Principle 4: Accurate and, where necessary, kept up to date.

Every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which it is processed, is erased, or rectified without delay.

360Giving will ensure that, wherever possible, all stored data will be reviewed and updated as necessary. 360Giving will not continue to keep data unless it is reasonable to assume that it is accurate. 360Giving's Data Protection Lead is responsible for ensuring that all staff are trained and understand the importance of collecting and maintaining accurate data. 360Giving's Data Retention Policy outlines how long data should be held for and subsequent procedures exist regarding the destruction and disposal of data and equipment. The following rules and guidelines are in place to ensure compliance with this principle:

- The Data Subject is also responsible for ensuring that data held by 360Giving is accurate and up to date
- All parties are required to notify 360Giving of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of 360Giving to ensure that any notification regarding change of personal data is recorded and acted upon at the earliest convenience

In line with this principle the Data Protection Lead is responsible for:

- Ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors
- Reviewing the retention dates, at least on an annual basis, of all the personal data processed by 360Giving
- Identifying any data that is no longer required (e.g. it is no longer required or used in line with the original intended purpose)
- Ensuring that data is securely deleted/destroyed in line with this policy
- Responding within one month to requests for rectification to personal data (i.e. where data is out of date/inaccurate) from Data Subjects
- Making appropriate arrangements to ensure that, where Data Processors, suppliers or third party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used and passing any correction to the personal data to the appropriate party as required

2.5 Principle 5: Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes, or

statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject.

Where personal data is retained beyond the retention date as outlined in 360Giving's Data Retention Schedule, 360Giving will investigate whether to:

- Minimise (i.e. delete certain data) personal data
- Encrypt the data
- Anonymise the data in order to protect the identity of the Data Subject(s)

Personal data will be retained in line with the Data Retention Policy and, once its retention date is passed, it must be securely destroyed as set out in this policy.

360Giving's Data Protection Lead must specifically approve any data retention that exceeds the retention periods defined in the Data Retention Policy, and must ensure that the justification is clearly identified and in line with the requirements of the GDPR. The approval of any data kept that exceeds any set retention periods must be written and documented.

2.6 Principle 6: Processed in a manner that ensures appropriate security

360Giving's Data Protection Lead will carry out a risk assessment taking into account all circumstances in relation to the control of and processing operations.

In determining appropriateness the Data Protection Lead will also consider the extent of possible damage or loss that might be caused to individuals (i.e. publishers, stakeholders etc) if a security breach occurs, the effect of the breach on 360Giving itself, and any likely reputational damage and loss of trust.

3. Accountability and Record-Keeping

3.1 360Giving's person responsible for our Data Protection activities (Data Protection Lead) is Tania Cohen, director@threesixtygiving.org.

3.2 The Data Protection Lead shall be responsible for overseeing the implementation of this Policy and for monitoring compliance with this Policy, 360Giving's other data protection-related policies, and with the GDPR and other applicable data protection legislation.

3.3 360Giving shall keep written internal records of all personal data collection, holding, and processing, which shall incorporate the following information:

3.3.1 The name and details of 360Giving, the person responsible for Data Protection, and any applicable third-party data processors;

3.3.2 The purposes for which 360Giving collects, holds, and processes personal data;

3.3.3 Details of the categories of personal data collected, held, and processed by 360Giving, and the categories of data subject to which that personal data relates;

3.3.4 Details of any transfers of personal data to non UK or EEA (European Economic Area) countries including all transfer mechanisms and security safeguards;

3.3.5 Details of how long personal data will be retained by 360Giving and

3.3.6 Descriptions of all technical and organisational measures taken by 360Giving to ensure the security of personal data.

4. The Rights of Data Subjects

The GDPR sets out the following rights applicable to data subjects (please refer to the parts of this policy indicated for further details):

- The right to be informed.
- The right of access;
- The right to rectification;
- The right to erasure (also known as the 'right to be forgotten');
- The right to restrict processing;
- The right to data portability;
- The right to object; and
- Rights with respect to automated decision-making and profiling.

4.1 Keeping Data Subjects Informed

4.1.1 360Giving shall provide the information set out in 4.1.2 below to every data subject:

a) Where personal data is collected directly from data subjects, those data subjects will be informed of its purpose at the time of collection; and

b) Where personal data is obtained from a third party, the relevant data subjects will be informed of its purpose:

- if the personal data is used to communicate with the data subject, when the first communication is made; or
- if the personal data is to be transferred to another party, before that transfer is made; or
- as soon as reasonably possible and in any event not more than one month after the personal data is obtained.

4.1.2 The following information shall be provided:

a) Details of 360Giving;

b) The purpose(s) for which the personal data is being collected and will be processed (as detailed in this Policy) and the legal basis justifying that collection and processing;

c) Where applicable, the legitimate interests upon which 360Giving is justifying its collection and processing of the personal data;

d) Where the personal data is not obtained directly from the data subject, the categories of personal data collected and processed;

e) Where the personal data is to be transferred to one or more third parties, details of those parties;

f) Where the personal data is to be transferred to a third party that is located outside of the UK or European Economic Area (the "EEA"), details of that transfer, including but not limited to the safeguards in place (see below for further details);

g) Details of data retention;

h) Details of the data subject's rights under the GDPR;

i) Details of the data subject's right to withdraw their consent to 360Giving's processing of their personal data at any time;

j) Details of the data subject's right to complain to the Information Commissioner's Office (the "supervisory authority" under the GDPR);

k) Where applicable, details of any legal or contractual requirement or obligation necessitating the collection and processing of the personal data and details of any consequences of failing to provide it; and

l) Details of any automated decision-making or profiling that will take place using the personal data, including information on how decisions will be made, the significance of those decisions, and any consequences.

4.2 Data Subject Access

4.2.1 Data subjects may make subject access requests ("SARs") at any time to find out more about the personal data which 360Giving holds about them, what it is doing with that personal data, and why.

4.2.2 Employees wishing to make a SAR should do so in writing to the fData Protection Lead.

4.2.3 Responses to SARs shall normally be made within one month of receipt, however this may be extended by up to two months if the SAR is complex and/or numerous requests are made. If such additional time is required, the data subject shall be informed.

4.2.4 All SARs received shall be handled by the Data Protection Lead.

4.2.5 360Giving does not charge a fee for the handling of normal SARs. 360Giving reserves the right to charge reasonable fees for additional copies of information that has already been supplied to a data subject, and for requests that are manifestly unfounded or excessive, particularly where such requests are repetitive.

4.3 Rectification of Personal Data

4.3.1 Data subjects have the right to require 360Giving to rectify any of their personal data that is inaccurate or incomplete.

4.3.2 360Giving shall rectify the personal data in question, and inform the data subject of that rectification, within one month of the data subject informing 360Giving of the issue. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

4.3.3 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of any rectification that must be made to that personal data.

4.4 Erasure of Personal Data

4.4.1 Data subjects have the right to request that 360Giving erases the personal data it holds about them in the following circumstances:

a) It is no longer necessary for 360Giving to hold that personal data with respect to the purpose(s) for which it was originally collected or processed;

b) The data subject wishes to withdraw their consent to 360Giving holding and processing their personal data;

c) The data subject objects to 360Giving holding and processing their personal data (and there is no overriding legitimate interest to allow 360Giving to continue doing so) (see below for further details concerning the right to object);

d) The personal data has been processed unlawfully;

e) The personal data needs to be erased in order for 360Giving to comply with a particular legal obligation.

4.4.2 Unless 360Giving has reasonable grounds to refuse to erase personal data, all requests for erasure shall be complied with, and the data subject informed of the erasure, within one month of receipt of the data subject's request. The period can be extended by up to two months in the case of complex requests. If such additional time is required, the data subject shall be informed.

4.4.3 In the event that any personal data that is to be erased in response to a data subject's request has been disclosed to third parties, those parties shall be informed of the erasure (unless it is impossible or would require disproportionate effort to do so).

4.5 Restriction of Personal Data Processing

4.5.1 Data subjects may request that 360Giving ceases processing the personal data it holds about them. If a data subject makes such a request, 360Giving shall retain only the amount of personal data concerning that data subject (if any) that is necessary to ensure that the personal data in question is not processed further.

4.5.2 In the event that any affected personal data has been disclosed to third parties, those parties shall be informed of the applicable restrictions on processing it (unless it is impossible or would require disproportionate effort to do so).

4.6 Data Portability

4.6.1 When 360Giving processes personal data using automated means, and where data subjects have given their consent to 360Giving to process their personal data in such a manner, or the processing is otherwise required for the performance of a contract between 360Giving and the data subject, data subjects have the right, under the GDPR, to receive a copy of their personal data and to use it for other purposes (namely transmitting it to other data controllers).

4.6.2 If applicable, requests for copies of personal data shall be complied with within one month of the data subject's request. The period can be extended by up to two months in the case of complex or numerous requests. If such additional time is required, the data subject shall be informed.

4.7 Objections to Personal Data Processing

4.7.1 Data subjects have the right to object to 360Giving processing their personal data based on legitimate interests, direct marketing (including profiling).

4.7.2 Where a data subject objects to 360Giving processing their personal data based on its legitimate interests, 360Giving shall cease such processing immediately, unless it can be demonstrated that 360Giving's legitimate grounds for such processing override the data subject's interests, rights, and freedoms, or that the processing is necessary for the conduct of legal claims.

4.7.3 Where a data subject objects to 360Giving processing their personal data for direct marketing purposes, 360Giving shall cease such processing immediately.

4.8 Automated Decision-Making

360Giving does not use personal data in automated decision-making processes – although professional contact information may be used as part of automated communications and reporting purposes.

4.9 Profiling

360Giving does not use personal data for profiling purposes.

5. Personal Data Collected, Held and Processed

See Appendix 1 for an overview of the personal data that is collected and processed by 360Giving, with details of retention.

6. Data Security

6.1 Transferring Personal Data and Communications

360Giving shall ensure that the following measures are taken with respect to all communications and other transfers involving personal data:

a) All emails containing personal data must be sent via encrypted threesixtygiving.org email account encrypted with Transport Layer Security (TLS);

b) All emails containing special category personal data must be marked "confidential";

c) Personal data may be transmitted over secure networks only; transmission over unsecured networks is not permitted in any circumstances;

d) Where personal data is to be transferred in hardcopy form it should be passed directly to the recipient.

6.2 Storage

360Giving shall ensure that the following measures are taken with respect to the storage of personal data:

a) All electronic copies of personal data should be stored securely using passwords and G-suite, which uses 128-bit or stronger Advanced Encryption Standard (AES) data encryption;

b) All hardcopies of personal data, along with any electronic copies stored on physical, removable media should be stored securely in a locked box, drawer, cabinet, or similar;

c) No personal data should be transferred to any device personally belonging to an employee and personal data may only be transferred to devices belonging to agents, contractors, or other parties working on behalf of 360Giving where the party in question has agreed to comply fully with the letter and spirit of this Policy and of the GDPR (which may include demonstrating to 360Giving that all suitable technical and organisational measures have been taken).

6.3 Disposal

When any personal data is to be erased or otherwise disposed of for any reason (including where copies have been made and are no longer needed), it should be securely deleted and disposed of.

6.4 Use of Personal Data

360Giving shall ensure that the following measures are taken with respect to the use of personal data:

a) No personal data may be shared informally and if an employee, agent, sub-contractor, or other party working on behalf of 360Giving requires access to any personal data that they do not already have access to, such access will be granted by the Data Protection Lead, as appropriate.

b) No personal data may be transferred to any employees, agents, contractors, or other parties, whether such parties are working on behalf of 360Giving or not, without the authorisation of the Data Protection Lead.

c) Personal data must be handled with care at all times and should not be left unattended or on view to unauthorised employees, agents, sub-contractors, or other parties at any time;

d) If personal data is being viewed on a computer screen and the computer in question is to be left unattended for any period of time, the user must lock the computer and screen before leaving it.

6.5 IT Security

360Giving shall ensure that the following measures are taken with respect to IT and information security:

a) All passwords used to protect personal data should be changed regularly and should not use words or phrases that can be easily guessed or otherwise compromised. All

passwords must contain a combination of uppercase and lowercase letters, numbers, and when possible symbols.

b) Under no circumstances should any passwords be written down or shared with agents, contractors. Passwords must only be saved in a secure password keeper service.

c) All software (including, but not limited to, applications and operating systems) shall be kept up-to-date. All staff shall be responsible for installing any and all security-related updates as soon as reasonably and practically possible, unless there are valid technical reasons not to do so, such cases approved IT support consultant should advise; and

d) No software may be installed on any 360Giving owned computer or device without the prior approval of the Data Protection Lead.

e) Automatic locking of desktop PCs and other equipment

f) Removal of access rights for USB and other memory media

g) Virus checking software and firewalls

h) Role-based access rights including those assigned to temporary staff

i) Encryption of devices that leave the organisations premises such as laptops

j) Security of 369Giving's technical networks

7. Organisational Measures

360Giving shall ensure that the following measures are taken with respect to the collection, holding, and processing of personal data:

7.1 All employees, agents, contractors, or other parties working on behalf of 360Giving shall be made fully aware of both their individual responsibilities and 360Giving's responsibilities under the GDPR and under this Policy, and shall be provided with a copy of this Policy;

7.2 Only employees, agents, sub-contractors, or other parties working on behalf of 360Giving that need access to, and use of, personal data in order to carry out their assigned duties correctly shall have access to personal data held by 360Giving;

7.3 All employees, agents, contractors, or other parties working on behalf of 360Giving handling personal data will be appropriately trained to do so;

7.4 All employees, agents, contractors, or other parties working on behalf of 360Giving handling personal data will be appropriately supervised;

7.5 All employees, agents, contractors, or other parties working on behalf of 360Giving handling personal data shall be required and encouraged to exercise care, caution, and discretion when discussing work-related matters that relate to personal data, whether in the workplace or otherwise;

7.6 Methods of collecting, holding, and processing personal data shall be regularly evaluated and reviewed;

7.7 All personal data held by 360Giving shall be reviewed periodically, as set out in 360Giving's Data Retention Policy;

7.8 The performance of those employees, agents, contractors, or other parties working on behalf of 360Giving handling personal data shall be regularly evaluated and reviewed;

7.9 All employees, agents, contractors, or other parties working on behalf of 360Giving handling personal data will be bound to do so in accordance with the principles of the GDPR and this Policy by contract – with disciplinary action measures for data breaches;

7.10 All agents, contractors, or other parties working on behalf of 360Giving handling personal data must ensure that any and all of their employees who are involved in the processing of personal data are held to the same conditions as those relevant employees of 360Giving arising out of this Policy and the GDPR; and

7.11 Where any agent, contractor or other party working on behalf of 360Giving handling personal data fails in their obligations under this Policy that party shall indemnify and hold harmless 360Giving against any costs, liability, damages, loss, claims or proceedings which may arise out of that failure.

These controls have been selected for consideration on the basis of identified risks to personal data, and the potential for damage or distress to individuals whose data is being processed.

8. Transferring Personal Data to a Country Outside the UK or EEA

8.1 360Giving may from time to time transfer ('transfer' includes making available remotely) personal data to countries outside of the UK or EEA.

8.2 The transfer of personal data to a country outside of the UK or EEA shall take place only if one or more of the following applies:

8.2.1 The transfer is to a country, territory, or one or more specific sectors in that country (or an international organisation), that the European Commission has determined ensures an adequate level of protection for personal data;

8.2.2 The transfer is to a country (or international organisation) which provides appropriate safeguards in the form of a legally binding agreement between public authorities or bodies;

8.2.3 The transfer is made with the informed consent of the relevant data subject(s);

8.2.4 The transfer is necessary for the performance of a contract between the data subject and 360Giving (or for pre-contractual steps taken at the request of the data subject);

8.2.5 The transfer is necessary for important public interest reasons;

8.2.6 The transfer is necessary for the conduct of legal claims;

8.2.7 The transfer is necessary to protect the vital interests of the data subject or other individuals where the data subject is physically or legally unable to give their consent; or

8.2.8 The transfer is made from a register that, under UK or EU law, is intended to provide information to the public and which is open for access by the public in general or otherwise to those who are able to show a legitimate interest in accessing the register.

9. Data Protection Impact Assessments

9.1 360Giving shall carry out Data Protection Impact Assessments for any and all new projects and/or new uses of personal data which involve the use of new technologies and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the GDPR.

9.2 Data Protection Impact Assessments shall be overseen by the Data Protection Lead and shall address the following:

- The type(s) of personal data that will be collected, held, and processed;
- The purpose(s) for which personal data is to be used;
- 360Giving's objectives;
- How personal data is to be used;
- The parties (internal and/or external) who are to be consulted;
- The necessity and proportionality of the data processing with respect to the purpose(s) for which it is being processed;
- Risks posed to data subjects;
- Risks posed both within and to 360Giving; and
- Proposed measures to minimise and handle identified risks.

10. Data Breach Notification and Policy

10.1 All personal data breaches must be reported immediately to the Data Protection Lead.

10.2 If a personal data breach occurs and that breach is likely to result in a risk to the rights and freedoms of data subjects (e.g. financial loss, breach of confidentiality, discrimination, reputational damage, or other significant social or economic damage), the Data Protection Lead must ensure that the Information Commissioner's Office is informed of the breach without delay, and in any event, within 72 hours after having become aware of it.

10.3 In the event that a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, the Data Protection Lead must ensure that all affected data subjects are informed of the breach directly and without undue delay.

10.4 Data breach notifications shall include the following information:

- The categories and approximate number of data subjects concerned;
- The categories and approximate number of personal data records concerned;
- The name and contact details of the person responsible for Data Protection (or other contact point where more information can be obtained);
- The likely consequences of the breach;
- Details of measures taken, or proposed to be taken, by 360Giving to address the breach including, where appropriate, measures to mitigate its possible adverse effects.

10.5 360Giving will keep a record of any incidents and breaches, whether reported or not, to demonstrate our accountability and learning from incidents and breaches to improve to improve our data management practices and security measures.

10.6 360Giving is required to report a breach to the Charity Commission in the following circumstances:

- Where data is accessed by unauthorised party/parties
- Equipment containing beneficiary or employee data has been lost/stolen
- Loss of funds due to phishing (e.g. giving bank account details online, by phone etc)
- A breach has occurred that has been reported to the ICO

Appendix 1 - Overview of the personal data collected and processed by 360Giving

Process Overview	Type of data	Data subjects	Retention
Payroll - remuneration, payroll and pension admin	Hard copy P45/46 employee payslips & P60s. Contact data for core tasks, pension admin.	Staff	Retained in line with staff privacy notice.
Recruitment	Electronic data for information entered into a CV or included in a cover letter, right to work documentation, references from former employers, criminal convictions.	Applicants (staff, Trustees and Committees)	Deleted in line with Applicant privacy notice.
Emergency contact	Contact details	Staff next of kin or other point of contact nominated by staff member.	Retained in line with staff privacy notice
Annual review and professional development	Contact details, comments on performance	Staff	Retained in line with staff privacy notice
Management of Contractors	Contact details, bank details.	External consultants	Contract and invoices retained are required to be kept for over 6 years.
Governance and Trustees	Contact details, trustee declarations.	Trustees	Retain in line with staff privacy policy
360Giving website	IP addresses, account details: name, email, job title, organisation name.	Website visitors, staff/consultants with CMS logins,	Stats are processed automatically and anonymously. User accounts retained as long as in use.
Newsletter contact list	Contact details, IP address (via Mailchimp)	Members of the public (who sign up); publisher contacts; other	Updates and cleaning made on ongoing basis. Each communication to include details for how to unsubscribe

		professional contacts	or update preferences/ contact details
Events management	Contact details	Publishers and other contacts	Participants' details retained as professional contacts.
Professional contact and engagement	Contact details	Publishers and other contacts	Participants' details retained as professional contacts.
Forum	Contact details, IP address	Anyone who visits or creates an account with 360 forum	Indefinitely - dormant users may be removed if required.
Data Champions Programme/ other training or programmes	Contact details Special Category Data	Applicants and participants	Participants' details retained as professional contacts. Special Category Data collected as part of the application process will be held separately and deleted within one month of offers being made.
360Giving support and publisher outreach	Contact details	Publishers and would-be publishers. Staff from target grantmakers	Participants' details retained as professional contacts.
Open data shared during preparation and feedback	Accidental personal data or individuals associated with a grant	unknown/ individuals receiving grant awards	Data files containing personal data deleted within one month after support has concluded.
Online tools functions	IP addresses, personal data in files	Website visitors, unknown subjects in open data	Pseudonymised IP addresses retained indefinitely or automatically deleted after 90 days.