Groundwork London

GDPR Policy and Procedure

May 2019

Policy Review

This policy and procedure will be regularly reviewed, and in the first instance after 6 months, and thereafter at a timescale to be determined

Version 1:	May 2018
Reviewed:	Nov 2018
	May 2019

Table of Contents

Data Protection Policy Statement

Groundwork London will uphold people's privacy rights and comply with legal and contractual obligations, while making effective use of personal data to support our charitable objectives.

Groundwork London will take a risk-based approach to data protection decision-making; keeping in mind the intent of data protection law and effective operational outcomes; adopting best recommended practice where there is ambiguity about minimal compliance requirements.

Data protection risk is ultimately owned by the Board of Trustees, with operational decisions delegated to the Executive Director as specified within is Data Protection Policy Framework.

Scope

This Policy applies to all “processing” of "personal data" (terms as defined by law)

- where Groundwork London is Data Controller, and
- where Groundwork London is Data Processor

Implementation

Our Data Protection Policy comprises of this Data Protection Policy Framework document and the supporting policies, procedures and guidance to which it refers to throughout.

The requirements of this Policy will be incorporated into the Groundwork London operational procedures and contractual arrangements.

A2: Our approach to accountability for managing personal data, for detail on the roles and responsibilities we have allocated to manage data protection risk.

Review

Groundwork London undertake to review the Policy and the latest best practice at least every 12 months. The Policy will also be reviewed when necessary – for example, in the event of legislative or organisational change.

Data Protection Fee – Registration

Groundwork London will pay the required data protection fee, and is registered with the Information Commissioner’s Office (ICO) with following reference: **Z9988876**

A: Accountability

A1: How we adhere to the data protection principles

A1.1: Lawfulness, fairness and transparency

We maintain a **records** which outlines our lawful basis for processing; processing of special categories of personal data, and processing of personal data relating to criminal convictions and offences

Section B2: Our approach to providing privacy information, details how we will fulfil our transparency obligations.

A1.2: Purpose limitation

This policy outlines our Business Objectives, the purposes for which we process personal data to deliver those Business Objectives, and a description of the processing activities we undertake for each.

When a new purpose for processing personal data is identified, we use the decision-making process described in A4.1.2: Our approach to re-using personal data.

A1.3: Data minimisation

The following sections describe how we implement the minimisation principle in day-to-day operations:

A4.1.1: Our approach to data minimisation

A4.1.2: Our approach to re-using personal data

A1.4: Accuracy

The following sections describe how we implement the accuracy principle

A4.1.3: Our approach to maintaining accurate personal data

B4.1: Our approach to implementing the right to rectification

A1.5: Storage limitation

The following sections describe how we implement the storage limitation principle

A4.1.4: Our approach to record retention and disposal

A4.1.5: Our approach to pseudonymisation and anonymisation

B4.2: Our approach to implementing the right to erasure

A1.6: Integrity and confidentiality

The following section describes how we implement appropriate security if personal data

C1: Our approach to managing the security of personal data

A2: Our approach to accountability for managing personal data

A2.1: Data Protection Officer (DPO) and other roles

We have assessed the criteria outlined in the GDPR and have concluded that we must appoint a DPO. This role is held by Michael Ronksley.

This decision is based on the following assessment:

Due to our wide ranging of projects, often on short contracts, we have a high turnover of staff and service users so we consider ourselves as needing a DPO. This is especially because much of the information is sensitive data (Article 9) and we work with vulnerable adults and store data relating to criminal convictions and offenses. (Article 10).

The Board of Trustees for Groundwork London is ultimately accountable for strategic approach to data protection.

The role of the Data Protection Officer is responsible for providing data protection oversight and expertise to the organisation as a whole.

The Data Protection Officer has operational responsibility for the organisation's good practice and will be accountable for maintaining the relevant records and Data Controller notification.

All staff, including volunteers, contractors and temporary workers, are required to understand and comply with data protection standards and procedures.

We will meet our accountability obligations by

(i) providing sufficient financial and other resources to enable this policy to be implemented.

(ii) ensuring that Strategic monitoring of data protection risk is overseen by the Data Protection Officer and is reported to Board of Trustees on a quarterly basis and when urgent risks arise.

(iii) Ensuring that Operational monitoring and reporting of data protection compliance will be carried out and recorded.

A2.2: Data protection training and awareness

We will conduct a training needs assessment to ensure all training and awareness is appropriate based on the nature, scope and context of the processing of personal data which is undertaken, and the data protection responsibilities of the role.

We will ensure staff receive data protection training and awareness by:

- Holding a GDPR session for all employees to attend which covers the changes to data privacy.
- Broaden the data privacy section for new staff inductions.
- Set a mandatory e-learning course to be completed by al new starters.
- Undergo 1:1s with departments and ensure they understand the level of awareness their staff require and train as accordingly to the needs of the project.
- Holding a quarterly review by a GDPR steering committee to assess needs of the company and provide additional support where required.
- Create auditing procedures to check staff have reached the require levels of understanding.

We will ensure volunteers receive data protection training and awareness by:

- Ensuring their line managers knows what their training requirements are for the role they are doing and know how to discuss this with staff and how to ensure their staff are compliant.
- Admitting them onto the e-learning if required.
- Ensuring they attend the new start induction where they are made aware of what their requirements are in the role and have a general understanding of GDPR.

A3: Our approach to working with suppliers and partners

When researching or negotiating with new suppliers, we ask them to sign an agreement confirming they meet the new data privacy requirements which includes the possibility of an audit.

We use standard Data Processor contract clauses for suppliers who are acting as Data Processors on our behalf.

When data is disclosed to other Data Controllers, we

Ensure they have signed our agreement template for handling our data

For ad-hoc arrangements we obtain email confirmation that a partner confirmed they are GDPR compliant before sharing data with them and record this in a dedicated inbox.

A4: Our approach to proactive management of Data Protection risk

A4.1: Data protection by design and default

Data protection by design and default will be embedded into our change and project management processes by training all department managers on what this is and how it works and asking them to assess all of their projects to ensure data is kept to a minimum. When launching new projects, these leads will be responsible for designing GDPR compliant projects and budgeting for it and these will be reviewed quarterly by the GDPR Committee.

A4.1.1: Our approach to data minimisation

When a purpose for processing personal data is identified, we will identify the processing activities required and design systems, data collection forms and processes to comply with the principle of minimisation.

Where there are multiple purposes with differing minimum data requirements, we will put in place suitable access controls and procedures to reduce excessive processing.

A4.1.2: Our approach to re-using personal data

If the re-use of personal data is for the same purpose as it was originally collected for then we will carry out the processing, ensuring that we adhere to

B1: Our approach to transparency and fairness to **individuals**.

If the re-use of personal data is for a new purpose then we assess whether the new purpose is compatible with the original purpose for which the personal data was collected by:

Example:

1. Referencing our policies to ascertain the original purpose and context of processing
2. Consulting data journey documents to determine the nature and scope of the processing
3. Determining whether a purpose compatibility assessment is required
4. Carrying out the assessment if required

A4.1.3: Our approach to maintaining accurate personal data

We adopt the following measures to maintain the accuracy of personal data:

For example:

- When a purpose for processing personal data is identified, we will identify the processing activities required and meet the level of accuracy required for the purpose (wherever personal data is collected, input, transferred or updated) by designing suitable systems, data collection forms and processes.

A4.1.4: Our approach to record retention and disposal

Our records retention process is to follow the retention periods required by our funders and partners where they are the Controllers. Otherwise we follow the legal retention periods, or those required for project delivery. We erase records at the earliest opportunity and this is reviewed quarterly by departments as reminded by the GDPR Committee which meet quarterly.

A4.1.5: Our approach to pseudonymisation and anonymisation

At the end of a project we will erase all personal data if it is no longer required. If we require it in some form, we will pseudonymise or anonymise where possible and we will not retain it longer than we have stated, unless we have sought permission from the data subject.

Going forward, projects will be designed so that data minimisation is borne in mind and data is pseudonymised or anonymised as early as possible, or not taken where extraneous.

A4.2: Data protection impact assessment

Before starting any high-risk processing activity, the decision as to whether a Data Protection Impact Assessment is required will be taken by the Data Protection Officer based on the criteria described in the GDPR and the Article 29 Working Party Guidance on Data Protection Impact Assessment.

A5: Our approach to transfers of personal data outside the EEA

The requirement for data to be transferred outside the European Economic Area will depend on the purposes of processing.

The condition for transfer will also be determined by the purpose.

We do not transfer data outside the EEA without a valid condition for processing and appropriate safeguards for the rights and freedoms of the data subjects.

Our process for ascertaining the appropriate condition for transfer and safeguards is ensuring that the provider has undergone an assessment by the GDP Committee or has signed our agreement confirming they are GDPR compliant.

B: Transparency

B1: Our approach to transparency and fairness to individuals

Our strategic approach to providing privacy information outlines

- the means (methods) we will use to provide privacy information, in order that this results in information that is accessible and can be comprehended by the different individuals (Data Subject Categories) we engage with, and

- how we will provide access to general privacy information, i.e. the privacy information that every Data Subject should be able to access.

B2: Our approach to providing privacy information

Our approach to providing privacy information to individuals is achieved by

- defining baseline of specific privacy information, and

- undertaking an assessment when required to define how privacy information will be provided to individuals.

B3: Our approach to providing individuals with access to their personal data

B3.1: Our approach to implementing the right of subject access

We ensure that data subjects are informed of their right to access their personal data and the options available to them for exercising this right by including this right in privacy information.

When a data subject access request is received, we log it, copy it to our GDPR email inbox and inform the DPO. Then the DPO will ensure the right people are tasked with delivering this information to the individual and logging the actions taken.

B3.2: Our approach to implementing the right of data portability

We ensure that data subjects are informed of their right to data portability where it applies, and the options available to them for exercising this right by including this right in privacy information.

When a request for data export or transfer for portability is received, we log it, copy it to our GDPR email inbox and inform the DPO. Then the DPO will ensure the right people are tasked with delivering this information in the right format to the individual and logging the actions taken.

B4: Our approach to enabling individuals to manage their personal data

B4.1: Our approach to implementing the right to rectification

We ensure that data subjects are informed of their right to rectification and the options available to them for managing their own data by including this right in privacy information.

When a request for rectification of inaccurate data is received, we

Log it, copy it to our GDPR email inbox and inform the DPO. Then the DPO will ensure the right people are tasked with rectifying the data held and will inform the individual and log the actions taken.

B4.2: Our approach to implementing the right to erasure

We ensure that data subjects are informed of their right to erasure, where it applies; by including this right in privacy information.

When a request for erasure of personal data is received, we

Log it, copy it to our GDPR email inbox and inform the DPO. Then the DPO will ensure the right people are tasked with erasing the data held and will inform the individual and log the actions taken.

B4.3: Our approach to implementing the right to restriction of processing

We ensure that data subjects are informed of their right to restriction of processing, where it applies to their personal data; by including this right in privacy information.

When an individual asserts the right to restriction, we

Log it, copy it to our GDPR email inbox and inform the DPO. Then the DPO will ensure the right people are tasked with restricting the use of data held and evaluate whether it could be erased and will inform the individual and log the actions taken.

B4.4: Our approach to implementing the right to object

We ensure that data subjects are informed of their right to object as it applies to their personal data; by including this right in privacy information.

Where processing is carried out under the lawful basis of legitimate interests or in the public interest; we will discuss with the individual what impact objecting will have on our service to them, and halt the processing, or erase their personal details as appropriate.

Where the objection is to the processing of personal data for direct marketing, we log it, and the project lead will restrict processing, or discuss deletion with the individual if this is more appropriate. The project lead will inform the individual and log the actions taken.

B4.5: Our approach to rights in relation to automated decision-making

When implementing processing which involves automated decision-making or profiling of individual which may have legal effects or similar, we will ensure that there are appropriate safeguards for the individuals' rights and freedoms by considering and building in those safeguards as described in A4.2: Data protection impact assessment

We ensure that data subjects are informed of their rights in relation to automated individual decision-making (including profiling) as it applies to their personal data; by including this right in privacy information.

When an automated decision is challenged, we will; immediately inform the DPO who will action accordingly. We do not currently make decisions by automated means, and if we do, the GDPR Committee or the DPO will institute a policy, guidelines and training around this activity to ensure compliance.

C: Security and personal data breaches

C1: Our approach to managing the security of personal data

The “nature, scope, context and purposes of processing” will come from the information obtained from our Data Flows. This information will be used to determine the “appropriate technical and organisational measures” that need to be taken in order to protect the personal data from unlawful or unauthorised processing and against accidental loss, destruction or damage.

C2: How we handle personal data breaches

C2.1: Our approach to managing security incidents

Guidance on how to recognise and report information security incidents is provided to staff and volunteers by training when they start, induction by their department managers, quarterly reminders from the GDPR Committee and guidance in the policy and staff handbook which all staff can access.

The process for investigating, reporting and responding to information security incidents is to report to a line manager and DPO and send to the GDPR email inbox for record keeping.

C2.2: Our approach to notifying the Supervisory Authority of a breach

Where an information security incident meets the definition of a “personal data breach” from Article 4 of the GDPR, an assessment is made as to whether there are sufficient mitigating measures in place to protect the rights and freedoms of the affected data subjects.

If the affected data subjects’ rights or freedoms may be affected by the breach, then the Information Commissioner’s Office will be notified.

This process is defined in our Data Breach Procedure which will be followed by the DPO in the event of a breach.

C2.3: Our approach to informing individuals of a security breach

Where an information security incident meets the definition of a “personal data breach” from Article 4 of the GDPR, an assessment is made as to whether there are sufficient mitigating measures in place to protect the rights and freedoms of the affected data subjects or whether there is a likelihood of high risk to their rights or freedoms as a result.

If there is a high likelihood that data subjects’ rights or freedoms will be affected by the breach then a communications plan for informing the affected data subjects will be implemented.

This process is defined in our Data Breach Procedure which will be followed by the DPO in the event of a breach.