Data Protection Policy

GP8 Data Protection Policy

1. POLICY STATEMENT

1.1 The aim of this policy statement is to give you a basic understanding of the data protection laws, our responsibility in respect of data protection practice, your rights and obligations and to explain why privacy is so important to us. It applies to all actions we take which involve the processing of and working with personal data.

1.2 This policy has been approved by the Board of Groundwork West Midlands.

1.3 In order to operate as an organisation we hold Personal Data about employees, suppliers, volunteers, customers, participants, and other individuals. The use of personal data is governed by the Data Protection Act (**Data Protection Act 2018**). We take data protection very seriously and understand the impact that data breaches and misuse of data may have on individuals whose data we hold (data subjects) as well as on our activities. Compliance with this policy is necessary for us to maintain the confidence and trust of those whose personal data we handle.

1.4 Non-compliance with this policy by employees could in certain circumstances constitute a serious disciplinary matter.

1.5 The aim of this policy statement is to give you a basic understanding of the data protection laws, our responsibility in respect of data protection practice, your rights and obligations and to explain why privacy is so important to us. It applies to all actions we take which involve the processing of and working with personal data. This policy has been approved by the Board of Groundwork West Midlands.

1.6 This policy has been approved by the Board of Groundwork West Midlands.

2 SCOPE

This policy applies to trustees, employees, consultants, volunteers, temporary/agency staff, volunteers and anyone acting on behalf of Groundwork West Midlands. In this policy, reference to "employee" includes reference to any consultants, volunteers, temporary / agency staff and anyone acting on behalf of Groundwork West Midlands.

3 DATA PROTECTION OFFICER (DPO) AND OTHER ROLES

We have assessed the criteria outlined in the Data Protection Act 2018 and have concluded that GWWM are not required to appoint a Data Protection Officer (DPO) and other roles **(See Appendix 1 Management of Key GDPR Requirements – Accountability summary)**

We have assessed the criteria outlined in the Data Protection Act 20118 and have concluded that GWWM are not required to appoint a DPO, but will allocate a role to be Data Protection Officer as Good Practice. This role is held by Andrew Thompson

Email; DPOWM@groundwork.org.uk
Address;
Data Protection Officer
Groundwork West Midlands
First Floor, Owen House
17 Unity Walk
DY4 8QLY
Tel: 0121 5305667

This decision is based on the following assessment:
That we are not:-

- a public authority
- an organisation that carries out the regular and systematic monitoring of individuals on a large scale
- Or an organisation that carries out the large scale processing of special categories of data, such as health records, or information about criminal convictions.

3.1. What do I need to know about Data Protection?

Data protection legislation is not intended to prevent processing of personal data but to ensure it is done fairly and lawfully and in a way which does not adversely affect an individual.

3.1.1 We will process your personal data in accordance with the data protection laws. Processing includes obtaining, recording, holding, reading, using or destroying personal data.

3.1.2 The Data Protection Act 2018 regulates the processing of personal data. Personal data is information relating to an identified or identifiable natural person. An identifiable natural person is someone who can be identified, directly or indirectly, in particular by reference to an identifier, which include names, identification numbers, location data or other factors such as the physical, genetic, biometric, mental, economic or social identity of a natural person. Data about businesses or organisations is not covered by the Data Protection Act 2018 but data about their directors, partners, employees, customers and suppliers is.

3.1.3 We will process personal data in accordance with the Data Protection Act 2018 and good

data protection practice and will only use personal data for the purpose(s) it was intended for. We will
Keep a processing record of all processing of personal data we perform. We will make sure our fair processing notices are up to date and reflect the processing activities we undertake.

3.1.4 We will store personal data in a safe and secure manner and only people who really need to use it as part of their work responsibilities will have access to it. We will keep personal data only as long as is necessary for the purpose(s) it was collected for. Once personal data is no longer required, we will take reasonable steps to delete, destroy or erase it.

3.1.5 We will keep personal data up to date. Where a data subject reports an inaccuracy in the personal data we hold, we will correct it (unless we know the information is correct) and will inform any recipients of that personal data of the amendments.

3.1.6 We will avoid collecting special categories of personal data or criminal data unless absolutely necessary. If we do collect it, we will take extra measures to ensure it is kept safe and secure in line with the training given

3.2. Keeping Data Secure - Our Record of Processing Activities (ROPA)

1.6.1. The ROPA is updated each time a new purpose of processing is identified, and a review of the lawful basis for that processing is carried out. The ROPA is reviewed for accuracy and currency by theme managers every quarter.

We will process personal data securely by ensuring the confidentiality, integrity and availability of personal data is kept secure. We will ensure the level of security we use is appropriate to the risks arising out of the processing.

1.6.2 We have put in place a variety of policies and procedures which will keep data secure by providing guidance for our staff and contractors as to how personal data should be stored in order to reduce, as far as reasonably possible, the risks involved in processing personal data.

1.6.3 We will work together with our IT team to ensure that where our staff needs to take electronic equipment containing personal data out of the office environment, the device contains security to keep the personal data safe and secure. **(See GP7 GWWM IT Policy).**

1.6.4 We have put in place other organisational and physical security measures to protect personal data. Staff and contractors must take particular care if they process personal data whilst working from home or away from the office. **(See GP7 GWWM IT Policy)**

1.7 Requests for data **(See Appendix 2 Data Subject Access Requests – Guidance)**

1.7.1 Individuals are entitled to make a request to us for a copy of the personal data that we hold about them. Requests should describe the information sought. Where we receive requests for personal data we will answer the request without undue delay and normally within one calendar month of receipt.

1.7.2 All data subject access requests will be considered properly. Should a request for data be received, we will

- Immediately inform the DPO who will arrange any initial response.
- The DPO with the appropriate Data Controller will ascertain the identity of the person requesting the rectification.
- The appropriate Data controller will investigate the request and subject to the identity check will action the response as appropriate.
- The Request will be recorded in the ROPA

1.7.3 If applicants are unhappy with the way we handle requests, they should let us know by completing a complaint form, a copy of which can be provided upon request from our Data Protection Officer.

1.7.4 Occasionally other bodies may ask for access to personal data we hold such as the police, the tax authorities and other enforcement agencies. Such requests should be referred to the Data Protection Officer.

1.8 Other rights

1.8.1 Data subjects have a number of rights including a right to erasure, a right to data portability, a right to object to certain processing, a right to restrict processing in certain circumstances and a right to prevent automated decision making in certain circumstances, a data subject may request that the processing of their personal data be restricted. If you receive such requests, please refer it to the Data Protection Officer

1.8.2 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, as documented in **(Appendix 3 - Privacy Information Strategy.)**

1.8.3 When a request for rectification of inaccurate data, erasure, restriction of processing, portability request or objection is received, we

- Immediately inform the DPO who will arrange any initial response.
- The DPO with the appropriate Data Controller will ascertain the identity of the person requesting the rectification.
- The appropriate Data controller will investigate the request and subject to the identity check will action the response as appropriate.
- The Request will be recorded in the ROPA

1.8.4 We are committed to ensuring data subject rights are upheld and we will work hard to make sure these rights can be exercised.

1.9 Sharing Data with other people/organisations

We will not send personal data to a third party or another organisation unless the data subject has given us their authority to do so or we are otherwise permitted by law. We will take care to consider whether the data subject has given authority to their data being passed to another organisation before we transmit the data. Where data is being sent to an organisation for them to process the data either on their own behalf or for us, we will carry out due diligence on that organisation to make sure they have adequate data protection standards and processes. We will carry out due diligence, put in place contracts and/or data sharing protocols to govern the use of data by the third party to ensure compliance with all relevant legislation and guidance.

1.10 Employee, Customer, Supplier, Tenant Data

In the course of normal business operations we will collect and process various personal data about employees, suppliers, customer, tenants, including special category personal data. This information will be retained for the period set out in the document and data retention policy. We will process this data in accordance with the relevant fair processing notices.

1.11 Training

We will provide all staff and temporary workers with appropriate data protection training to make sure that data protection issues are dealt with properly and in accordance with this policy and the law. We will make sure staff, temporary workers and workers at our processors have adequate

training for their roles.

1.12 Data Retention and Destruction

Personal data will be retained by us as long as we need to process it or for as long as the law requires us to keep it. When we no longer need data we will delete or destroy it in accordance with good data protection practice. Where we use third party contractors to delete or destroy data, we will only use contractors who can demonstrate relevant experience and accreditations. ***(See GP11* GWWM Records and Archiving Management Policy).**

1.13 Data breaches

A data breach is a breach of security which leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to, personal data transmitted, stored or otherwise processed. In the event of a data breach, the Data Protection Officer shall log the breach, deal with it and resolve any issues arising out of the breach. **(*See Appendix 4 Personal Data Breaches)*.**

1.14 Transferring Data Outside the European Economic Area (EEA)

We do not intend to transfer personal data outside the EEA. Where it is necessary to do so we will ensure any such transfer is carried out in accordance with the requirements of the **Data Protection Act 2018 and the GDPR** to ensure that the level of protection to data subjects guaranteed by the **Data Protection Act 2018** is not undermined by any such transfer.

As the United Kingdom has left the European single market, we shall ensure that any transfer of personal data overseas is transferred in accordance with all applicable data protection legislation in place at the time of such transfer.

1.15 Changes to this Policy

We reserve the right to change this policy at any time where it is appropriate for us to do so; we will notify individuals of these changes.

In the event that the United Kingdom leaves the European single market, we will ensure that we comply with any new data protection legislation that is enacted as a result.

Groundwork West Midlands Ltd undertake to review the Policy and the latest best practice at least every 3 years. The Policy will also be reviewed when necessary – for example, in the event of legislative or organisational change.

1.16. Data Protection Fee – Registration

Groundwork West Midlands Ltd will pay the required data protection fee, and is registered with the Information Commissioner's Office (ICO) with following reference **Z1885772**

1.17 Authorisation

This Data Protection Policy Statement has been adopted by the Groundwork West Midland Board of Trustees as follows:

Monitoring and Review

This policy will be monitored on a regular basis and will be reviewed in accordance with legislative requirements.

Approved by: Executive Director January 2025
Updated by: Office Manager, HR Advisor, Groundwork West Midlands, January 2025
Review date: In line with current legislation or every three years (January 2028)

Appendix 1 Management of Key Data Protection Act 2018 Requirements –Accountability summary

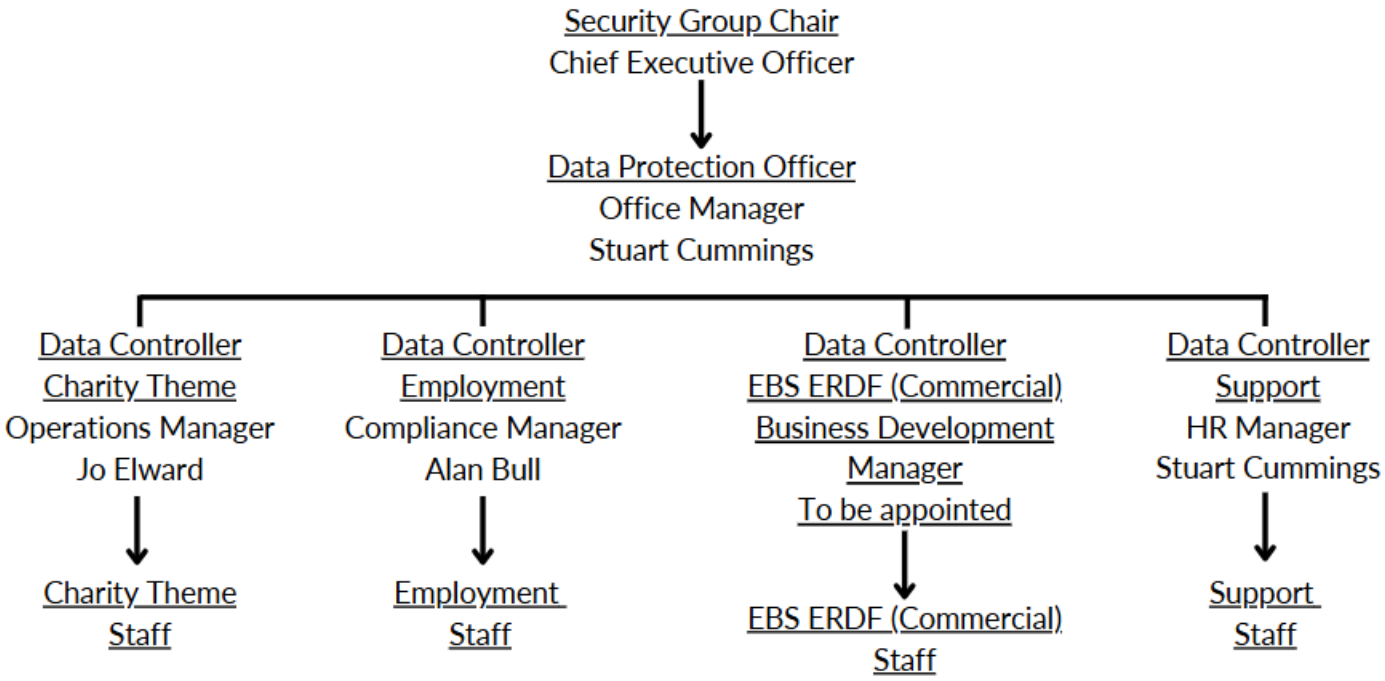
This document details the structure of Data Controllers for GWWM and their area of accountability.

The management of Data and the control and security of that data is managed in the same structure at the line management within the staffing structure of GWWM

There are 4 main themes covered by the structure with appropriate Heads of Theme or agree Data Controllers in place and accountable for the Data and Control of that Data for their appointed areas.

The structure and accountability is therefore as follows:

Diag. 1



The Data Controllers for the Themes, as shown in Dig. 1 will be responsible for:-

- Arranging the ROPA for their appropriate area of responsibility,
- Ensuring that the ROPA is regularly updated and kept current with staffing changes and project work.
- Ensuring that the IT Manager is informed of any changes to permissions to folder access.
- Will carry out appropriate Audits on their staff to ensure that agreed controls and systems are being followed.
- Will ensure that all the relevant Privacy notices and Privacy information strategy is maintained.
- Will ensure that suitable security arrangements are in place for the security of all physical folders and files.
- Ensure that clear desk policies and arrangements are in place for their staff.

Security Group

The Security Group comprises all the company Directors, DPO and Data Controllers.

The Security Group, chaired by the CEO will have oversight over all Electronic and Physical data they will:-

- Organise and arrange Audits
- Monitor Audit results and approve appropriate action to rectify any shortfall
- Receive reports from the DPO and Data Controllers and approve appropriate actions.

The Security Group will meet Bi-Monthly or when required

Audit and compliance

All staff who work with Personal Data or Sensitive Personal Data will be subject to regular audits (minimum – 6 monthly) of their workstations and processes. These should be carried out by line managers who are familiar with the work processes of the staff in question.

The audits and finding will be monitored and recorded at the Security Group Meeting.

Appendix 2 Data Subject Access Requests – Guidance

Data Subject Access Requests – Guidance

Under Data Protection Act 2018 people (Data Subjects) have the right to access their information and we need to be certain that we can deal with these requests.
However GWWM can sometimes be seen to operate as 4 distinct business
Charity
Employment
Commercial (EBS & ERDF)
Support

Unfortunately people contacting us from the outside sometimes do not know who they need to talk to and in the case of Data Protection Act 2018 and Data Subject Access Requests (DSAR's) they may contact someone in the wrong department.

However the new Data Protection Regulations 2018 put a time limit on us responding to requests and that starts the moment a Data Subject (The caller) contacts us and so it is very important that the correct information is collected and emailed to me the Data Protection Officer immediately at

DPOWM@groundwork.org.uk

I will take on the request from there with the appropriate Data Controller but I must know about it first.

Please obtain as must information as you can

- Name
- Contact telephone Number or numbers
- Email Address
- Address
- The basics of what the request is about:-
    - If old staff when they worked for us and department
    - If a client what project did they attend or participate in

I or a Data controller will then contact then and let them know how we will respond to their request as it may be just for Information, that information they think we have is wrong, that they wish to be removed from out files.

Some of this is quite complicated and will require time to sort and so we will also tell them an expected outcome time.

Can we ask an individual for ID?

If you have doubts about the identity of the person making the request you can ask for more information. However, it is important that you only request information that is necessary to confirm who they are. The key to this is proportionality.
You need to let the individual know as soon as possible that you need more information from them to confirm their identity before responding to their request. The period for responding to the request begins when you receive the additional information.

Appendix 3 Privacy Information Strategy.

Privacy Information Strategy for Groundwork West Midlands

Data controllers will be responsible for ensuring that all Data subjects receive full and adequate Privacy information in line with the Guidance supplied by the ICO and agreed with the Groundwork West Midlands Security Group.

Details of what Privacy Notices have been used will be included in the appropriate section of the ROPA and full copies of all Privacy Notices used will be retained in the Library of Privacy Notices and any revisions will be recorded by date changed or revised and noted on the ROPA as changed that date

Privacy Information – Guidance on Privacy Notes From ICO

The starting point of a privacy notice should be to tell people:

- who you are
- what you are going to do with their information
- who it will be shared with

These are the basics upon which all privacy notices should be built. However, they can also tell people more than this and should do so where you think that not telling people will make your processing of that information unfair. This could be the case if an individual is unlikely to know that you use their information for a particular purpose or where the personal data has been collected by observation or inference from an individual's behaviour.

Map your information processing (ROPA)

To help you decide what you need to include you should map out how your information flows through your organisation and how you process it, recognising that you might be doing several types of processing. You should work out:

- what information you hold that constitutes personal data
- what you do with the personal data you process
- what you actually need to carry out these processes - a privacy impact assessment can help you to answer this question
- whether you are collecting the information you need
- whether you are creating derived or inferred data about people, for example by profiling them
- whether you will be likely to do other things with it in the future – this can be particularly important if you are undertaking large scale analysis of data, as in big data analytics

When explained in sufficiently broad terms a privacy notice can allow for development in the way you use personal data, whilst still providing individuals with enough detail for them to understand what you will do with their information. However, you should not draw up a long list of possible future uses if, in reality, you do not intend to process personal data for those purposes.

Go beyond legal requirements

Depending on the circumstances, you may decide it is beneficial to go beyond the basic requirements of the law, for example by telling people:

- the links between different types of data you collect and the purposes that you use each type of data for
- the consequences of not providing information - for example, non-receipt of a benefit
- what you are doing to ensure the security of personal information;
- information about their rights of access to their data
- what you will not do with their data

If you are relying on consent, you should:

- display it clearly and prominently
- ask individuals to positively opt-in
- give them sufficient information to make a choice
- explain the different ways you will use their information, if you have more than one purpose
- provide a clear and simple way for them to indicate they agree to different types of processing
- include a separate unticked opt-in box for direct marketing.

Actively give privacy information if:

- you are collecting sensitive information
- the intended use of the information is likely to be unexpected or
- objectionable
- providing personal information, or failing to do so, will have a
- significant effect on the individual
- the information will be shared with another organisation in a way
- that individuals would not expect

Write and present it effectively:

- use clear, straightforward language
- adopt a style that your audience will understand
- don’t assume that everybody has the same level of understanding
- as you
- avoid confusing terminology or legalistic language
- draw on research about features of effective privacy notices
- align to your house style
- align with your organisation’s values and principles
- be truthful. Don’t offer people choices that are counter-intuitive or
- misleading
- follow any specific sectoral rules
- ensure all your notices are consistent and can be updated rapidly
- provide separate notices for different audiences

Appendix 4 Personal Data Breaches.

How we handle personal data breaches

Our approach to managing security incidents

Guidance on how to recognise and report information security incidents is provided to staff

- Through the EduCare induction process and ongoing EduCare training

The process for investigating, reporting and responding to information security incidents is

- Immediately inform the DPO who will arrange any initial response.
- The incident will be recorded on the ROPA regardless of confirmation
- The DPO with the appropriate Data Controller will investigate fully the suspected breach and confirm what further action is to be taken.
- Should the breach require notification to the ICO it will be carried out by the DPO within the allocated 72 hours
- The DPO and Appropriate Data controller will continue to investigate until a resolution is found.
- The DPO will be responsible for coordinating and notifying any Data Subjects of the breach.
- All actions will be recorded on the ROPA

Our approach to notifying the Supervisory Authority of a breach

Where an information security incident meets the definition of a "personal data breach" from the Data Protection Act 2018, 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.

- The ICO will be notified by the DPO by completing the online report through https://ico.org.uk/for-organisations/report-a-breach/

Our approach to informing individuals of a security breach

Where an information security incident meets the definition of a "personal data breach" from the Data protection Act 2022, 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.

- The DPO and appropriate Data Controller will assess the most appropriate means of contacting the Data Subject dependent upon the information held by GWWM
- Whenever possible a letter will be sent recording all the evidence and actions relevant to the Breach to the Data Subject on completion of any investigation.