GEM Data Protection Policy and Procedures

GEM needs to keep certain personal data relating to individuals that it works with, including individuals signing up as members of the organisation, as well as personal data on funders, employees, volunteers, trustees and other partners and suppliers. This information is kept only to the extent necessary to enable us to carry out our day to day operations and meet our statutory obligations.

The organisation is committed to ensuring any personal data is dealt with in line with applicable data protection legislation (including the General Data Protection Regulation ["GDPR"] when that comes into force on 25 May 2018). To comply with this legislation, personal data will be collected and used fairly, stored safely and not disclosed to any other person or organisation unlawfully.

This document highlights key data protection requirements at GEM and aims to ensure that all employees, volunteers and trustees act in accordance with relevant legislation.

1. Definitions and Principles

1.1. Glossary of terms used in this policy

Personal data – information which relates to a living individual from which the individual can be identified including opinions or expressions of intention towards the individual on the part of GEM. Photographs, films and audio files are classified as personal data if they enable the identification of a specific individual or individuals. Personal data can also include electronic data such as IP addresses or location data, as well as physical data in paper records.

Sensitive personal data – information that relates to certain characteristics of an individual such as gender, religion, political affiliations, information relating to mental or physical health or biometric information.

Processing data – means obtaining, using, holding, amending, destroying or deleting personal data. This includes information stored in paper-based filing systems as well as electronic files.

1.2. Data principles

The GDPR (and prior legislation) requires that data shall be:

- Processed lawfully, fairly and transparently.
- Collected and processed for a specific, explicit and legitimate purpose.
- Relevant and limited to the purpose for which it is being processed.
- Accurate and kept up to date; every effort should be made to rectify or erase inaccurate or out of date data.
- Kept in a form that permits the identification of the data subject for no longer than is necessary for the purpose for which the data was collected and processed.
- Kept appropriately secure.

1.3. Data subject rights

Data subjects, including employees, have certain rights under the GDPR in relation to the data that an organisation holds on them. These rights include:

- The right to make a written request to access data held by GEM.
- The right to have any inaccurate data rectified.
- The right to have data erased.
- The right to restrict processing of any data.
- The right to data portability.
- The right to object to the use of personal data.
- The right to withdraw consent.

2. Types of personal data collected at GEM

The following are categories of personal data collected by GEM:

Trustees: contact information (email addresses, phone numbers, addresses), information contained in CVs and job application forms, notes from interviews, references, management information, bank details, equal opportunities monitoring information, mixture of electronic and paper records.

Minutes of Trustee meetings: may include personal information including identifiable opinions.

Staff members and freelancers: contact information (email addresses, phone numbers, addresses), information contained in CVs and job application forms, notes from interviews, references, management information, bank details and other payroll information, equal opportunities monitoring information, mixture of electronic and paper records.

Members of GEM, including applicants to join, groups of named individuals within organisations that join as institutions, individuals whose memberships have expired/lapsed: contact information (names, email addresses, phone numbers, addresses).

Job applicants: information supplied on CVs, application forms, cover letters and references.

Volunteers: contact information (email addresses, phone numbers, addresses), bank details (on expenses forms), information contained on CVs, references, management information, notes from interviews, equal opportunities monitoring information.

GEM publications, newsletter and mailing list subscribers: names, addresses, phone numbers and email addresses.

Partners and funders: names, addresses, phone numbers and email addresses.

Contributors to the GEM website events/freelancers/resources listings system: contact information (email addresses, phone numbers and addresses).

Supplier information: including contact details and bank account information.

Project participants: contact information including reports and identifiable opinions on the activity they undertake in partner projects.

Customers, including those attending workshops and conferences, audiences and charitable donors: contact information (email addresses, phone numbers, addresses), bank details.

3. Registration with the ICO

GEM is registered with the ICO as a data controller.

GEM will ensure compliance with this registration including submitting an annual return to the ICO. The Director will be responsible for this function.

4. Responsibilities

Overall responsibility for personal data processed by GEM rests with the Board of Trustees. The Board of Trustees delegates the following tasks to the Director (who in turn may delegate where appropriate):

- Understanding and communicating obligations under the Data Protection Act 1998, GDPR and any other relevant legislation.
- Identifying potential risks around data collection, processing and storage.
- Producing clear and effective procedures.

All staff, trustees and volunteers who process personal information must read this policy and ensure they understand its implementation and the eight data protection principles outlined above.

Breach of this policy will result in disciplinary proceedings.

The maximum penalties for failure to comply with GDPR are a fine of 20 million euros or 4% of global turnover whichever is the larger amount.

5. Implementation

5.1. Collecting new data, processing data and updating existing data

In collecting any new data and processing any existing data held, GEM will be relying on its legitimate interest or on express consent:

- Consent – under the GDPR consent must be freely given, specific, informed and unambiguous. There must be a clear affirmative action involved in giving consent. Consent has to be verifiable and individuals have certain rights if they give consent to a data controller.

- Legitimate interest – include direct marketing, transferring employee data for administrative purposes, ensuring information security. If legitimate interest is being relied upon, this has to be clearly stated in an information notice, an assessment of the legitimate interest vs the rights of the data subject has to be recorded and the data subject has the rights to object.

Note children have a special set of rights under the GDPR. For the purposes of the GDPR a child is anyone under the age of 16. Parental consent is required to process a child's data. Please consult the Board of Trustees if a project requires us to hold children's personal data.

When planning to collect new personal data for processing, staff members, trustees and volunteers should check the Information Asset Register to ensure that we do not already hold the data required.

Name of asset	Format	Where held	Personal data (note if related to children)	Lawful basis and note of how determined	Retention period

If the data being collected is new or additional data to that which we already hold, the following questions should be considered:

- What will the information be used for and is this a legitimate purpose in the context of the operation of GEM? See below for further analysis of this question.
- Who needs to access the information once it has been collected?
- How will it be stored?
- How long will it be kept for and how will we ensure continuing accuracy?
- What is the lawful basis for processing the data?

If the staff member, volunteer or Trustee then goes ahead with the decision to collect the data, a new entry for that category or group of data should be made in the Information Asset Register.

If they are collecting data that is similar to a type already noted in the Information Asset Register, they should note the basis for processing and check that it is still applicable. If the basis for processing has changed an appropriate amendment or new entry to the register should be made.

If data is being collected or processed on the basis of Legitimate Interest, a brief note of the grounds for that decision should be recorded in the Register.

If data is being collected on the process of consent, a note of where the consent is recorded should be made in the register.

If there is any data being collected from under 16s this should be noted and a record made that it meets the additional requirements for collecting data from this age group.

5.2. Collecting and processing data on the basis of legitimate interest

Examples of legitimate interest:

- Where there is a reasonable expectation that a person's data will be processed.
- Where there is an appropriate relationship between the data controller and the individual.

Both of these examples could reasonably be true of staff from organisations that have an existing relationship with GEM, for example if they have signed up as a member or participated in a GEM project.

Other areas where legitimate interest could be an appropriate basis for holding and processing data:

- Employee relations
- Web analytics
- Partnership working

If Legitimate Interest is identified as the most likely lawful basis for processing, we must conduct a Legitimate Interest Assessment to confirm that this is appropriate.

The Legitimate Interest Assessment should consider:

- What is the legitimate interest?
- Is pursuing the legitimate interest necessary for achieving the legitimate interest identified (is there another way to do it that doesn't involve disproportionate effort for example)?
- When the legitimate interest is balanced with the rights of the individuals whose data is being processed, the rights of the individuals are not disproportionately harmed by pursuing the legitimate interest.

The Legitimate Interest Assessment should be carried out by the member of staff or volunteer collecting the data and signed off by the Director. The results should be noted on the Information Asset Registered a copy of the test should also be filed in our secure server.

If the Legitimate Interest Assessment shows that we cannot rely on Legitimate Interest, then steps should be considered to modify the scope of the data being collected or processed to make this possible. If modifying the scope does not enable us to use Legitimate Interest then an alternative basis for data processing must be sought.

Informing Data Subjects:
If we are using Legitimate Interest as a basis for processing, this information must be communicated to the data subjects. This could happen in a privacy notice or privacy statement.

5.3. Collecting and processing data using Consent

If you have chosen Consent as the basis for collecting and processing data, there should be a clear way for a data subject to give their consent at the point at which the data is being collected. This should be separate from any other terms, conditions or instructions that are presented.

In obtaining consent it has to be clear:

- What the data will be used for.
- That the person is clearly and freely giving their consent by an affirmative action (e.g. ticking a box, filling in details, replying to an email requesting consent).
- What a person should do if they wish to withdraw their consent.
- Information about how your data will be treated – link to Privacy Policy.

Consent needs to be clearly recorded. The record of consent needs to include:

- What they have consented to.
- How they were informed about what they consented to.
- How they consented.
- Date consent was given.

Consent should be granular ie you are only asking people to consent to one thing at once.

This needs to be updated if consent is subsequently withdrawn.

Consent should be recorded as directed by the Director.

5.4. Collecting data from under-16s

We should strive to minimise the amount of data we hold and process from children under the age of 16.

The GDPR states that children under 16 cannot give consent for their data to be processed. The consent of a parent or guardian is required. This must be taken into account if consent is the basis on which we are holding data from under-16s.

6. Data Storage and Retention

6.1. Storage

The GDPR says that all data must be stored in a way that is appropriately secure. This applies to data that is stored electronically and data that is stored on paper.

6.1.1. Electronic Storage

The requirement to use all IT equipment in a manner that is compatible with secure data storage is outlined in the staff handbook and computer user policies. Anyone who has a GEM phone, laptop or tablet that is regularly used away from the office is asked to sign a Laptop User Form that outlines their responsibility for storing and using the device securely.

The aim is for GEM to have implemented a CRM database in 2018/19. When this database is in place, the following should be taken into consideration in respect of storage of all data:

- Personal data should be stored in the most secure way possible. Consideration should be given to who needs to access data and when they need to have access.
- Spreadsheets containing personal data should be password protected; only one copy of any spreadsheet should be maintained.
- Spreadsheets containing personal data should not be emailed.
- Personal data held by GEM should not be taken away from our offices except in case of a specific need (ie an offsite event where it is necessary to take contact details of attendees). Any details taken off-site should be stored and disposed of securely.
- Emails should not, if possible, be a system for storing personal data.
- If personal data is held on memory sticks they should be password protected or ideally encrypted and stored securely.
- Personal data should not be stored on personal devices.

6.1.2 Physical Storage

- Personal data held on paper should be stored securely in locked drawers or cupboards. Access to these should be restricted to those who require access to the data.
- Any documents used by individual staff members or volunteers that contain sensitive data should not be left on desks overnight. They should either be put away in desk drawers (ideally lockable) or locked in one of the cupboards.
- Paper copies of personal data should not be removed from the office unless it is necessary for business purposes – ie a copy of an event guest list with delegate contact details. This data should be securely disposed of after use. Paper copies of personal data must not be stored away from the office in employees' homes or other locations.

6.2 Retention

The GDPR specifies that data should only be held for as long as is necessary for the purpose it was collected for.

General principles for data storage

- Governing documents, information relating to charity governance such as minutes of board meetings: in perpetuity.
- Financial documents, bank documents, Gift Aid documents: six years after the end of the accounting period to which they relate.
- Contracts with suppliers and funders: six years.
- Insurance documents: permanently.
- Operating documents, project documents (business plan, management accounts): one year.
- HR documents – relating to interviews (staff and volunteer): one year, names and addresses only retained for three years.
- HR documents – relating to former staff: six years after employment ceases.
- Pensions records: permanently.
- Data should be kept as up to date as possible – if someone contacts us to tell us their details have changed, we must change them promptly.
- Deletion or disposal of personal data should be done securely ie shredding paper documents.

7. Data Subject Rights

Under the GDPR, data subjects have the following rights:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

In practice this means anyone has the right to be informed about what data GEM holds on them and how we are processing it.

In most cases, we have to respond to any requests for information within one calendar month of the request being made.

Data has to be provided in an accessible format, free of charge.

GEM has the right to refuse to comply with the request or charge an administrative fee if the request is repetitive or excessive.

8. Data Breaches

A data breach is a breach in security which leads to the destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

Things that could lead to a data breach include:

- Weak / stolen passwords
- Lost / stolen devices
- Malware attacks

In the event of a data breach:

- It is not mandatory to report the loss unless there is a risk to individual data subjects' rights.
- Any data breach should be reported to the Director who will then consult with the Chair of Trustees to make an assessment of severity.
- In the event the breach is determined to be severe, it must be reported to the ICO within 72 hours of occurring.
- As soon as the data breach is discovered an appropriate plan needs to be put in place to rectify the problem.
- As soon as the data breach is discovered a communications plan needs to be put in place to inform the affected individuals about what has happened to their data.
- All actions taken in response to a data breach must be recorded, this responsibility will rest with the Director.

9. Enquiries

All questions from staff, volunteers and trustees relating to data protection should be directed to the Director.

10. Awareness Raising

All GEM staff, freelancers, volunteers and Trustees are required to read this policy when they join GEM. Biannual reminders about data protection will be given.

A large amount of practical guidance including examples is available on the ICO website https://ico.org.uk/for-organisations/business/

11. Review

This policy will be updated in line with relevant changes in legislation.

If there are no significant changes to the law, this policy will be reviewed every two years and updated if necessary.