A4 Data Protection Policy

Appendix 1 Data Breach Procedure

1. Purpose

1.1. This document outlines the process for reporting suspected data breaches involving personal data, including data thefts or exposures (including unauthorised access use, or disclosure) and to outline the response to a confirmed, data breach, theft or exposure based on the data involved.

1.2. A personal data breach can cause immense personal distress. Our priority is to safeguard and protect the rights and freedoms of those who trust us with their personal data, mitigate the impact of an identified breach and in so doing maintain compliance with data protection legislation.

2. Scope

2.2. This policy applies to all personal and sensitive personal data processed by GFS and anyone acting on behalf of the organisation as defined by the Data Protection Act. 1998 and the General Data Protection Regulations, 2018

2.3. It includes paper based documents and filing systems, electronic data, including equipment containing personal data such as mobile phones, tablets and laptops.

3. Data Processors

3.1. GFS uses data processors to administer a range of its services and functions such as payroll and criminal records checks. If a data processor suffers a breach to its systems that affects personal data, it is required by law to notify GFS as soon as it becomes aware.

4. Data Manager

4.1. The data manager is responsible for notifying the Information Commissioner's Office (ICO), following notification of a serious breach, investigating a breach and taking appropriate measure to address the breach including where necessary notifying the data subject (individual).

4.2. The GFS Operations Manager will act as the data manager. The post holder is responsible for ensuring compliance with GFS data protection policies and procedures, risk management and record keeping.

5. Information Commissioner's Office

5.1. The Information Commissioner is an independent body that upholds information rights in the public interest. It has powers to take action where an organisation fails to comply with data protection legislation. It is empowered to defend the consumer interest including;

- Performing a data protection audit
- Levy a fine for use of data other than the purpose for which it was originally collected
- In cases of serious data breaches fines of up to 20 million euro or 4% of annual turnover.

5.2. These sanctions apply to all sectors and organisations including charities.

6. Personal and Sensitive Personal Data

6.1. GFS collects personal and sensitive personal data and is committed to ensuring its systems and processes protect the privacy of all who participate in our activities, and who work for and on behalf of GFS.

6.2. Data is personal if it relates to an identifiable living individual data and can be collected and processed manually and electronically.

6.3. There are special categories of personal data also referred to as **sensitive personal data**. Unauthorised disclosure of this information has the potential to have a more serious and detrimental impact on an individual.

6.4. During the course of our activities GFS may collect;

- The racial or ethnic origin of the data subject
- The subject's religious beliefs or beliefs of a similar nature
- Information on the subject's physical or mental condition
- Information on the subject's sexual life
- The commission of, or an alleged commission of, an offence by the data subject
- Information relating to the commission or alleged commission of an offence by the data subject

7. Personal Data Breach

7.1. The ICO defines a personal data breach as;

'A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data. This includes breaches that are the result of both accidental and deliberate causes'

8. Examples:

- Sending personal data to an incorrect recipient e.g. (email to wrong person)

- Lost equipment (computer, or mobile phone being lost or stolen)
- Personal data accessed by an unauthorised third party
- Alteration of personal data without permission

9. Action to be taken in the event of a data breach

9.1. Where a data breach relating to the loss of personal data is known or suspected prompt action is required to protect the rights and freedoms of the individual(s) affected.

9.2. The following actions must be taken by the person discovering the breach to minimise the risk to the individual and severity of its impact.

Step 1. Containment

The immediate priority is to contain the breach wherever possible and limit the scope of its impact. This will depend on the;

- The type and extent of personal information
- The number of people affected

Step 2. Inform the Data Manager

If you discover a personal data breach you **must** notify the data manager **within 24 hours** email: operations@girlsfriendlysociety.org.uk

Please complete the online GFS Data Breach template with as much detail as possible including;

- **When the breach (or suspected breach) occurred**
  - E.g. time and date (approximate)
  - Where you were at the time

- **Description of the type of personal information involved**
  - E.g. the categories of personal data
  - Names, telephone numbers, emergency contact, health information,
  - number of people affected

- **The reason for the breach (if known) or how it was discovered**
  - E.g. Phone stolen/lost, email error, left on train, unauthorised access (who) (how)

- **Identify which system has been or may have been affected**
  - E.g. Email account, mobile phone, was it password protected is it backed up, photocopies, repeated conversation suggesting breach, can it be restored,

- **Whether you have taken any corrective action to remedy or ameliorate the impact of the breach**
  - E.g. Tried to recall email, get the data back in another way, deactivate phone, contact train station, changed password.

10. Risk Management

10.1. The data manager will review all data breaches and will be responsible for notifying the ICO as appropriate.

10.2. The data manager will take reasonable steps to notify the individual affected by the breach. This will be determined on a case by case basis as not all breaches may require notification.

10.3. The data manager will co-ordinate an investigation and may seek additional information from the person identifying the breach, staff, volunteers and data processors.

10.4. The investigation may also include;

- A review of the type of information affected
- How sensitive it is
- The number of people affected
- Whether a third party could tell anything about the data subject from the information.

10.5. Following an assessment of the breach including risks to the individual and the organisation, the data manager will put in place a recovery plan.

10.6. GFS is a learning organisation and will take steps to review training, guidance and support following a data breach. In addition, any recommended changes to systems and process will be recorded and reported for action.

10.7. The data manager will update the organisation's risk register and report serious incidences to the Board of Trustees.

END