POLICY DOCUMENT

Policy	**Data Protection**
Policy Number	**A4**
Implementation Date	**May 2018**
Review Date	**May 2019**
Reviewed By	**Data Manager**
Connecting Policies	**All**

1. Introduction

1.1. In order to carry out its work and meet operational, safeguarding and legal obligations GFS administers personal information about; staff, volunteers, girls and young women as well as parents, donors, members and others.

1.2. GFS undertakes to protect all personal information held and ensure it is used in accordance with the provisions of the Data Protection Act 1998 and General Data Protection Regulations 2018.

1.3. This policy applies to all staff, volunteers and those responsible for processing personal data on behalf of GFS. It sets out the organisation's approach to data protection and provides information and guidance for processing personal data.

2. Personal Data

2.1. Personal data is information that relates to a living individual who can be identified from that data directly or indirectly. It relates to information processed by automatic means (electronic data) and paper based records including filing systems.

3. Data Protection Principles

3.1. In order to process personal data GFS adheres to the following data protection principles.

Personal data;

3.2. **must be processed fairly and for a lawful purpose**;
3.3. **must be collected for specified, explicit and lawful purpose;**
3.4. **must not be processed in a way that is incompatible with the original purpose**;

any personal information given or received in confidence for one purpose may not be used for a different purpose or passed on to anyone else without the consent of the data subject;

3.5. **should be adequate and relevant in relation to the purpose for which it was originally processed.** Individuals who input or update information must ensure that it is unambiguous and professional. Matters of opinion (not fact) must be clearly recorded as such.

3.6. **must be accurate and where necessary kept up to date.** It is the responsibility of those who receive personal information to ensure, so far as possible, that it is correct, valid and up to date.

3.7. **should not be kept longer than is necessary** for the purposes for which it was originally processed; (please refer to the attached record keeping schedule), Any personal data held must be reviewed at frequent intervals to ensure that it is accurate, up to date and still relevant. If the personal data held is no longer needed and there is no legal or other reason for holding the information, it should be destroyed.

3.8. **must be processed in accordance with the rights of the data subject**

4. Special Category Data

4.1. Special category data refers to personal information that is particularly sensitive in nature as the impact of unauthorised disclosure on a person's rights and freedoms could potentially be catastrophic.

4.2. Special category information may include information about a person's;

- race;
- ethnic origin;
- religion;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.
- criminal record

4.3. GFS will comply with the additional conditions governing the processing of special category data as set out in GDPR Article 9 (2) sections 9(a), (b), (c)(d) and (h) to ensure;

- Explicit consent is sought and given
- Processing is necessary for exercising legal obligations e.g. employment law and safeguarding,
- Processing is necessary to protect the vital interests of the data subject
- Processing is carried out in the course of GFS' legitimate activities.

5. Individual Rights

5.1. It is important that whenever GFS collects personal data that it does so correctly.

5.2. Everyone has rights to;

- understand what personal information is being processed;
- access their personal data
- rectify their personal data
- erase personal data
- restrict processing
- data portability
- object to processing
- rights in relation to decision making and automatic profiling.

6. Children and Young People

6.1. GFS processes personal information about children and young people to ensure they receive the right information, advice and support when accessing our services.

6.2. Personal information is collected from children and young women and attracts a legal duty of confidence until it has been effectively anonymised.

6.3. This legal duty (established under common law) prohibits information use and disclosure without consent – effectively providing individuals with a degree of control over who sees information they provide in confidence. This duty can only be overridden if there is a statutory requirement, a court order, or if there is a robust public interest justification.

6.4. GFS may collect;

- Name, address, date of birth, telephone, mobile
- Relevant family information
- Medical and emergency data
- Photographs, drawings and other visual images
- Email communications
- Social Media communications (e.g. Facebook)
- Professional judgements, opinions and comments about child
- Health and safety records (including accidents)
- Referral information
- Child protection notes
- Things that have happened whilst taking part in activities
- Things other people say about the children and young women

6.5. Such information may be captured at registration, for a particular event, such as a trip out. It may be processed via paper based or electronic mediums such as email, mobile phone, PC, or laptop.

6.6. GFS will inform children and young women about the use of and access to their personal data.

6.7. This means fully describing how the personal information will be used i.e. what will be done to the information; for what purposes it will be used, who it will be passed onto, how it will be processed, stored and destroyed.

6.8. GFS will ensure this has been explained understood and signed consent obtained and recorded.

7. Volunteer Data

7.1. GFS holds personal data about perspective and approved volunteers. The information is held to ensure appropriate checks are carried out to enable them to work with children, communicate information and provide support and development.

7.2. Special category or sensitive information related to a criminal record check is processed and expressed consent is obtained for this purpose. The information is shared with the data processor administering criminal records checks currently CCPAS.

7.3. GFS does not retain personal information processed as a part of criminal records check. Personal data may also be shared with training providers for which consent will be sought.

8. Donor Data

8.1. GFS benefits from donations from its members and the public in support of our work. Personal data about a donor is used to process the donation.

9. Staff Data

9.1. GFS processes personal information about job applicants, as well as current and former employees covering all stages of the employees' work with the organisation.

9.2. GFS may supply personal information to other organisations who are data processors such as for payroll processing. It may also share information with third parties e.g. where a former employee seeks a reference request.

10. Subject Access Request

10.1. GFS acknowledges the rights of the individual to be informed about what personal data the organisation holds about them. The formal term for requesting this information is a subject access request.

10.2. In addition, an individual has a right to be:

- Given a description of the personal data, why it is being processed, whether it will be given to any other organisation or people,
- Given a copy of the personal data, and
- Given details of the source of the data
- A right to prevent processing likely to cause them substantial damage or distress or significantly to prejudice their rights and freedoms;

- A right to prevent processing for the purposes of direct marketing
- A right to stop automated decision-taking
- A right to have incorrect data rectified, blocked, erased or destroyed

10.3. The GFS SAR procedure sets out roles, responsibilities and the procedure for managing requests.

11. Security of Personal data:

11.1. For GFS maintaining the security and confidentiality of personal data is of the utmost importance therefore staff, volunteers and trustees must understand the importance of ensuring personal data is secure and adhere to these principles.

- Personal data relating to members and volunteers should be securely stored on the volunteer/members data base
- Different rights of access should be allocated to different users depending on their role description
- Sending sensitive personal data by email should be an exception unless encrypted
- Leavers should be removed from all systems without delay, passwords changed, permissions revoked, and all equipment returned.
- A clear desk policy should be adopted in order to reduce any potential unauthorised access to paper records containing personal information.
- All IT equipment is password protected in order to keep personal data secure. IT users have to create their own password in order to log onto IT equipment. This password needs to be difficult for others to guess so family/pets names should be avoided.
- Passwords should contain a combination of upper and lower case letters and numerals, which should be changed regularly.
- Passwords must not be written down or disclosed to anyone else.
- All files and personal information must be in a locked cabinet when not in use.
- Files should never be left unattended or found in a visible or accessible place to visitors or other young women.
- Computer records must never be left on a laptop computer.

11.2. Staff/volunteers are required to carry limited sensitive data when on an offsite trip for emergency contact purposes.

11.3. This would include:

- The young person's name and contact details on their consent form
- Emergency contact details
- Their medical information and doctor's details
- This information should be kept safe by the lead staff/volunteer member for the trip and should be securely destroyed on completion of the trip.

11.4. The transportation of personal data in any format (laptop, hard copy, memory stick etc.) for any other reason should be avoided as far as possible. It is especially important to avoid carrying sensitive personal data, large volumes of personal information, or information which could cause particular harm or distress if lost.

11.5. If in exceptional circumstances information does have to be carried, it must not be left unattended or in any way be accessible to third parties.

12. Sharing Information

12.1. Effective information sharing is a vital element of both early intervention and safeguarding and GFS have adopted the six key principles outlined in the Government Guidance on Information Sharing as highlighted within the Child and Vulnerable Adult Protection Policy (A3).

12.2. Information on specific children and young women should only be discussed with staff/volunteers for the purposes of risk assessment and safety and when relevant.

12.3. For example, if two or more branches/groups are coming together for an activity and they need to share medical or behavioural information about an individual.

12.4. If it is appropriate to share information about particular girls or young women for learning purposes, e.g. on a training course, the child or young woman must be kept anonymous.

12.5. Staff or volunteers should refrain from engaging in social discussions about children or young women known to them including mentioning personal or confidential information about individuals.

12.6. All records must be available to the appropriate senior staff member as required.

12.7. When working with third parties while supporting children and young women any information shared must be recorded on the Information Sharing Record (ISR11)

13. Disclosing Information with Consent

13.1. As a general principal personal information should only be disclosed with the consent of the young woman or person with parental responsibility. A record must be kept of their consent.

13.2. For consent to be legally valid it must be:

- Freely given, without threat or pressure
- Informed consent – sufficient information is provided so that a young person genuinely understands what they are consenting to
- Specific – there should be clarity about who you can disclose to and for what purpose

14. Disclosing Information Without Consent

14.1. There are however, exceptional circumstances where confidentiality cannot be maintained.

14.2. Confidentiality **cannot** be offered in matters of child and vulnerable adults protection. The person who receives such information should handle the situation sensitively and explain that it is necessary to involve other agencies in order to protect the child and/or vulnerable adult.

14.3. Although agreement should generally be sought, the situation may arise where information has to be shared with other agencies without the child/young person's/adult's agreement or that of their parent.

14.4. In some circumstances, e.g. suspicion of sexual abuse, it may be necessary to share information without first informing the child or their parent/carer. Staff and volunteers must discuss these situations with the safeguarding lead who will decide the course of action.

14.5. In addition, the following areas in which an individual's personal information may be disclosed without consent are:

- **Missing Person**. It is sufficient to inform police to say that the person is safe.
- **Crime within the organisation.** If a crime occurs on any service premises or during any event or activities.
- **Serious offences.** In limited circumstances, if it is known or believed that a serious crime has been committed confidentiality can be breached
- **Possession of dangerous implement/substance**. Information should be disclosed if you have information that the young women/family member/partner is in possession of an implement such as a knife or substance, that from the information given to you indicates it is going to be used to harm another.

14.6. The decision to use an exemption from the non-disclosure provisions i.e. to share or not share information must be recorded and agreed with the relevant line manager. Advice must be sought from the director, or safeguarding lead.

15. Confidential Information

15.1. Confidentiality does not mean secrecy; rather it is about having a professional approach to handling and disclosure of information. All trustees, staff and volunteers must be able to draw a distinction between information, which others need to be aware of for the benefit of GFS and those who use our services, and the right of children and young women and others to confidentiality.

15.2. GFS' work should not be discussed with the media other than as set out in the procedures for dealing with the press and media.
15.3. Information obtained during the course of employment as a staff member or work as a committee member or volunteer should not be used

for personal gain or benefit, nor should it be passed on to others who might not use it on such a way.

16. Data Breach

16.1. The Information Commissioners Office (ICO) is responsible for ensuring all organisations comply with data protection regulations. It is empowered to impose severe financial penalties where the regulations are not adhered to.

16.2. 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.'

16.3. Our primary responsibility is to protect the rights and freedoms of the individual concerned and immediate steps will be taken to contain, remedy or ameliorate the impact of the breach.

16.4. A serious breach will be reported to the ICO in accordance with statutory provisions.

16.5. Incidents, including 'near misses', that affect confidentiality, integrity or availability of information and lead to the unauthorised destruction, denial, disclosure or modification of information, must be reported to the data manager.

16.6. The data breach procedure sets out the process for managing a breach. This must be seen as a way of improving procedures and awareness whilst eliminating poor practices and carelessness, rather than apportioning blame.

17. Privacy Impact Assessment

17.1. A Privacy Impact Assessment is a process that enables an organisation to identify privacy risks of a new policy or proposal. It enables an organisation to check the legitimacy of the proposed use of personal data and identify what consents should be put in place.

17.2. This is a good practice model that will be put in place at GFS to minimise privacy risks for all who work with us.

18. Training

18.1. Induction will include training and information on data protection and confidentiality. All staff are to undertake awareness training which reflects their role and responsibility within the organisation.

18.2. It is the responsibility of the relevant manager to ensure that volunteers understand and comply with the requirements of this policy and participate in training in line with the needs of the organisation.

End