Data Protection Policy including GDPR, Subject access requests and data breach protocols.

Standing in the Gap. Registered charity no: 1174627

Postal address: Ferndown House, Milton Road, Bloxham, Banbury, OX15 4HD

www.sitgap.org

Contents

1. Introduction

The Data Protection Act 2018 covers information about individuals which is held on computer or in a manual filing system, or which is recorded with the intention that it will be part of such systems. The Act applies to people or organisations that use or hold such personal data.

The Act is based on the right of the individual (the Data Subject) to know what information is being held about them, and how the information will be used. The Act sets out principles to ensure that personal data is:

- used fairly, lawfully and transparently
- used for specified, explicit purposes
- used in a way that is adequate, relevant and limited to only what is necessary
- accurate and, where necessary, kept up to date
- kept for no longer than is necessary
- handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

There is stronger legal protection for more sensitive information, such as:

- race
- ethnic background
- political opinions

- religious beliefs
- trade union membership
- genetics
- biometrics (where used for identification)
- health
- sex life or orientation

There are separate safeguards for personal data relating to criminal convictions and offences.

Standing in the Gap holds personal information on trustees, staff, volunteers, and service users.

Standing in the Gap seeks to comply with both the letter and the spirit of the Act.

The designated data protection officer for Standing in the Gap is: Bobbie Brown

2. Scope of the policy

- Staff and volunteer personal records will be kept at Standing in the Gap in accordance with its procedures
- Standing in the Gap staff and volunteers, other than the Clinical Director, will only have access to information which is relevant for the work they undertake within Standing in the Gap
- When trustees, staff and volunteers leave, all personnel documents will be kept in accordance with Standing in the Gap's Records retention procedure (see Appendix 2)
- To ensure data security all trustees and staff are required to complete the GDPR security checklist (Appendix 3) this is then stored in a locked filing cabinet.
- Trustees, Staff, Volunteers and clients have the right to see the information held on them by Standing in the Gap. To do this they should follow the Subject Access Request procedure as found in Appendix 1.
- Information about individuals will not be disclosed to any third party outside of Standing in the Gap without the permission of the individual, unless there is a significant risk to a child or vulnerable adult as identified in the Standing in the Gap safeguarding policy.
- In the case of a data breach, the Data breach procedure should be followed (Appendix 4).
- Where photographs of staff and/or volunteers are used to publicise or promote the organisation, permission will be sought from individuals and the photograph used for a specified length of time.

This policy is to be read in conjunction with the following policies/documents:

- Safeguarding Policy
- Whistle-blowing Policy

Appendix 1: Subject Access Request Procedure

This procedure is to be followed when an individual contacts Standing in the Gap to request access to their personal information held by the Charity. Requests must be completed within 1 month, so it should be actioned as soon as it is received. SAR's should be provided free of charge, however, a 'reasonable fee' may be charged when a request is manifestly unfounded or excessive, particularly if it is repetitive.

The steps below should be followed to action the request:

1. Is it a valid subject access request?
    a) The request must be in writing (letter, email, social media or fax).
    b) Has the person requesting the information provided you with sufficient information to allow you to search for the information? (You are allowed to request for more information from the person if the request is too broad.)

2. Verify the identity of the requestor.
    a) You must be confident that the person requesting the information is indeed the person the information relates to. You should ask for the person to attend the office with their passport/photo driving licence and confirmation of their address (utility bill/bank statement).

3. Determine where the personal information will be found
    a) Consider the type of information. (Personal data is data which relates to a living individual who can be identified from the data (name, address, email address, database information) and can include expressions of opinion about the individual.)
    b) If you do not hold any personal data, inform the requestor. If you do hold personal data, continue to the next step.

4. Screen the information
    a) Some of the information you have retrieved may not be disclosable due to exemptions, however legal advice should be sought before applying exemptions. Examples of exemptions are:
        - References you have given
        - Publicly available information
        - Crime and taxation
        - Management information (restructuring/redundancies)
        - Negotiations with the requestor
        - Regulatory activities (planning enforcement, noise nuisance)
        - Legal advice and proceedings
        - Personal data of third parties
5. Are you able to disclose all the information?
    a) In some cases, emails and documents may contain the personal information of other individuals who have not given their consent to share their personal information with others. If this is the case, the other individual's personal data must be redacted before the SAR is sent out.

6. Prepare the SAR response (using the sample letters at the end of this document) and make sure to include as a minimum the following information:

    a) the purposes of the processing;

    b) the categories of personal data concerned;

    c) the recipients or categories of recipients to whom personal data has been or will be disclosed.

    d) where possible, the envisaged period for which personal data will be stored, or, if not possible, the criteria used to determine that period;

    e) the existence of the right to request rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

    f) the right to lodge a complaint with the Information Commissioners Office ("ICO");

    g) if the data has not been collected from the data subject: the source of such data;

    h) the existence of any automated decision-making, including profiling and any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

    Be sure to also provide a copy of the personal data undergoing processing.

All SAR's should be logged to include the date of receipt, identity of the data subject, summary of the request, indication of whether Standing in the Gap can comply, date information is sent to the data subject.

Sample letters:

Replying to a subject access request providing the requested personal data

"[Name] [Address]

[Date]

Dear [Name of data subject]

Data Protection subject access request

Thank you for your letter of *[date]* making a data subject access request for *[subject]*. We are pleased to enclose the personal data you requested.

Include 6(a) to (h) above.

Copyright in the personal data you have been given belongs to the Charity or to another party. Copyright material must not be copied, distributed, modified, reproduced, transmitted, published or otherwise made available in whole or in part without the prior written consent of the copyright holder.

Yours sincerely"

Release of part of the personal data, when the remainder is covered by an exemption

"[Name] [Address]

[Date]

Dear [Name of data subject]

Data Protection subject access request

Thank you for your letter of *[date]* making a data subject access request for *[subject]*. To answer your request we asked the following areas to search their records for personal data relating to you:

- [List the areas]

I am pleased to enclose *[some/most]* of the personal data you requested. *[If any personal data has been removed]* We have removed any obvious duplicate personal data that we noticed as we processed your request, as well as any personal data that is not about you. You will notice that *[if there are gaps in the document]* parts of the document(s) have been blacked out. *[OR if there are fewer documents enclose]* I have not enclosed all of the personal data you requested. This is because *[explain why it is exempt]*.

Include 6(a) to (h) above.

Copyright in the personal data you have been given belongs to the Charity or to another party. Copyright material must not be copied, distributed, modified, reproduced, transmitted, published, or otherwise made available in whole or in part without the prior written consent of the copyright holder.

Yours sincerely"

Replying to a subject access request explaining why you cannot provide any of the requested personal data

"[Name] [Address]

[Date]

Dear [Name of data subject]

Data Protection subject access request

Thank you for your letter of *[date]* making a data subject access request for *[subject*].

I regret that we cannot provide the personal data you requested. This is because *[explanation where appropriate]*.

[Examples include where one of the exemptions under the data protection legislation applies. For example the personal data might include personal data is 'legally privileged' because it is

contained within legal advice provided to the Charity or relevant to on-going or preparation for litigation.

Other exemptions include where the personal data identifies another living individual or relates to negotiations with the data subject.

If necessary Standing in the Gap will seek appropriate expert advice before responding.

Yours sincerely”

Appendix 2: Records Retention Procedure

Standing in the Gap recognises that the efficient management of its records is necessary to comply with its legal and regulatory obligations and to contribute to the effective overall management of the association. This document provides the policy framework through which this effective management can be achieved and audited.

It covers:

- Scope
- Responsibilities
- Retention Schedule

Scope

This policy applies to all records created, received or maintained by Standing in the Gap in the course of carrying out its functions. Records are defined as all those documents which facilitate the business carried out by Standing in the Gap and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received or maintained in hard copy or electronically. A small percentage of Standing in the Gap records may be selected for permanent preservation as part of the Charity's archives.

Responsibilities

Standing in the Gap has a corporate responsibility to maintain its records and record management systems in accordance with the regulatory environment. The person with overall responsibility for this policy is the Data Protection Officer. The person responsible for records management will give guidance for good records management practice and will promote compliance with this policy so that information will be retrieved easily, appropriately and in a timely manner. Individual staff and employees must ensure that records for which they are responsible are accurate, and are maintained and disposed of in accordance with Standing in the Gap records' management guidelines.

Retention Schedule

The retention schedule refers to record series regardless of the media in which they are stored.

Document	Minimum Retention Period	Reason
Minutes		
Minutes of committee meetings	Indefinite	Archive as required by the Charity Commission
Employment		
Staff employment contracts	6 years after ceasing employment	Management
Staff payroll information	3 years	Management
Staff references	6 years after ceasing employment	Management

Application forms (interviewed – unsuccessful)	6 months	Management
Application forms (interviewed – successful)	6 years after ceasing employment	Management
Disciplinary files	6 years after ceasing employment	Management
Staff appraisals	6 years after ceasing employment	Management
Finance		
Receipt and payment accounts	6 years	VAT
Bank statements	Last completed audit year	Audit
Cheque book stubs	Last completed audit year	Audit
Paid invoices	Last completed audit year	VAT
Paid cheques	Last completed audit year	Limitation Act 1980
Payroll records	3 years	HMRC
Petty cash accounts	Last completed audit year	Audit
Insurance		
Insurance policies	6 years after policy end	Management
Certificates for Insurance against liability for employees	6 years after policy end	Management
Certificates for Public Liability	6 years after policy end	Management
Insurance claim records	6 years after policy end	Management
Health and Safety		
Accident books	3 years from date of last entry	Statutory
Risk assessment	3 years	Management
General Management		
Trustees contact details	Duration of membership	Management

Lease agreements	12 years	Limitation Act 1980
Contracts	6 years	Limitation Act 1980
Email messages	At end of useful life	Management
Consent forms	5 years	Management
GDPR Security Compliance form	Duration of membership	Management

Appendix 3: GDPR Security Compliance Checklist

All Trustees and staff should complete the security checklist below to show compliance. Records should be retained whilst they remain in office.

	Yes/No
Computer is password protected	
Email is password protected	
Mobile devices are password protected	
Flash drives are password protected	
External hard drives are password protected	
G Suite access is password protected	
Hard copy files are held securely	
Anti-virus software is up to date	
No one outside the Standing in the Gap has access to your Standing in the Gap information	

Data compliance will not be achieved if you have answered “No” to any of the above:

Name: _____

Signature: _____

Date: _____

Appendix 4: Data Breach Procedure

GDPR defines a personal data breach as "a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". Examples include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a controller or processor
- Sending personal data to an incorrect recipient
- Computing devices containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data

Standing in the Gap takes the security of personal data seriously, computers are password protected and hard copy files are kept in locked cabinets.

Consequences of a personal data breach

A breach of personal data may result in a loss of control of personal data, discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of personal data, damage to property or social disadvantage. Therefore a breach, depending on the circumstances of the breach, can have a range of effects on individuals.

Standing in the Gap to report a breach

If the data breach is likely to result in a risk to the rights and freedoms of the individual, the breach must be reported to the individual and ICO without undue delay and, where feasible, not later than 72 hours after having become aware of the breach. The Data Protection Officer must be informed immediately so they are able to report the breach to the ICO in the 72 hour timeframe.

If the ICO is not informed within 72 hours, Standing in the Gap via the DPO must give reasons for the delay when they report the breach.

When notifying the ICO of a breach, Standing in the Gap must:

i. Describe the nature of the breach including the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned
ii. Communicate the name and contact details of the DPO
iii. Describe the likely consequences of the breach
iv. Describe the measures taken or proposed to be taken to address the personal data breach including measures to mitigate its possible adverse affects.

When notifying the individual affected by the breach, Standing in the Gap must provide the individual with (ii)-(iv) above.

Standing in the Gap would not need to communicate with an individual if the following applies:

- It has implemented appropriate technical and organisational measures (i.e. encryption) so those measures have rendered the personal data unintelligible to any person not authorised to access it;
- It has taken subsequent measures to ensure that the high risk to rights and freedoms of individuals is no longer likely to materialise, or
- It would involve a disproportionate effort

However, the ICO must still be informed even if the above measures are in place.

Data processors duty to inform Standing in the Gap

If a data processor (eg. payroll provider) becomes aware of a personal data breach, it must notify Standing in the Gap without undue delay. It is then Standing in the Gap's responsibility to inform the ICO, it is not the data processor's responsibility to notify the ICO.

Records of data breaches

All data breaches must be recorded whether or not they are reported to individuals. This record will help to identify system failures and should be used as a way to improve the security of personal data.

Record of Data Breaches

Date of breach	Type of breach	Number of individuals affected	Date reported to ICO/individual	Actions to prevent breach recurring

To report a data breach use the ICO online system:

https://ico.org.uk/for-organisations/report-a-breach/