Data Protection Policy

Contents

1. Introduction

Birmingham & Solihull Women's Aid (BSWA) obtains, uses, stores and otherwise processes personal data relating to:

- potential, current and former staff, trustees and volunteers;
- service users, including children and young people;
- perpetrators of domestic abuse;
- potential, current and former commissioners, funders, donors and partners;
- website users and contacts

Collectively, the above are referred to in this policy as data subjects. When processing personal data, BSWA is obliged to fulfil individuals' reasonable expectations of privacy by complying with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act (2018) and other relevant data protection legislation.

BSWA takes its responsibilities with regard to the management of the requirements of the GDPR very seriously. This policy sets out how BSWA manages those responsibilities. All staff, trustees and volunteers processing personal data on BSWA's behalf must read and adhere to this policy. Failure to do so may result in disciplinary action

2. Purpose

This policy seeks to ensure that we:

- comply with the data protection law and with good practice;
- protect the rights of staff; service users; donors and partners
- are clear about how personal data must be processed and BSWA's expectations for all who process personal data on its behalf;
- protect BSWA's reputation by ensuring the personal data entrusted to us is processed in accordance with data subjects' rights
- protect BSWA from risks of personal data breaches and other breaches of data protection law.

The main terms used are explained in the glossary at the end of this policy (Annex A)

3. Scope

This policy applies to all personal data and special categories of personal data processed by BSWA and as defined underthe GDPR, including personal data held in electronic and paper-based filing systems; CCTV and image libraries.

Personal Data means any information relating to an identified or identifiable living individual. Identifiable living individual means a living individual who can be identified

or who are identifiable, directly from the information in question; or who can be indirectly identified from that information in combination with other information.

This can include:

- names of individuals;
- postal addresses;
- email addresses;
- telephone numbers;
- online identifiers, such as IP addresses and cookie identifiers.

3.1 The lawful bases

The lawful bases for processing are set out in Article 6 of the UK GDPR. Whenever BSWA processes personal data, one of the following must apply:

Consent: the individual has given clear consent for their personal data to be processed for a specified purpose

Contract: the processing is necessary for a contract BSWA has with the individual, or because a contract and Data Sharing Agreement is in place with a partner who has obtained the necessary lawful consents.

Legal obligation: the processing is necessary for BSWA to comply with the law (not including contractual obligations).

Vital Interests: the processing is necessary to protect someone's life.

Public task: the processing is necessary for BSWA to perform a task in the public interest or for official functions, and the task or function has a clear basis in law.

Legitimate interests: the processing is necessary for BSWAs legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

3.2 Special Categories of Personal Data

The UK GDPR defines special category data as:

- personal data revealing **racial or ethnic origin**;
- personal data revealing **political opinions**;
- personal data revealing **religious or philosophical beliefs**;
- personal data revealing **trade union membership**;
- genetic data;
- **biometric data** (where used for identification purposes);
- data concerning **health**;
- data concerning a person's **sex life**; and
- data concerning a person's **sexual orientation**.

Special category data includes personal data revealing or concerning the above types of data. Therefore, if BSWA staff have inferred or guessed details about someone which fall into one of the above categories, this data may also count as special category data and must be processed as such.

To ensure the processing of special category data is lawful, an Article 6 (above) basis for processing must be identified in addition to one of the specific conditions in Article 9 of the UK GDPR:

a) the data subject has given explicit consent to the special category data collection;
b) the processing is necessary in the context of employment law, or laws relating to social security and social protection;
c) the processing is necessary to protect vital interests of the data subject or of another natural person;
d) the processing is carried out in the course of the legitimate activities of a charity or not-for-profit body, with respect to its own members, former members, or persons with whom it has regular contact in connection with its purposes;
e) the processing relates to personal data which have been manifestly made public by the data subject;
f) the processing is necessary for the establishment, exercise or defence of legal claims, or for courts acting in their judicial capacity;
g) the processing is necessary for reasons of substantial public interest, and occurs on the basis of a law that is proportionate to and protects the rights of data subjects;
h) the processing is required for the purpose of medical treatment undertaken by health professionals, including assessing the working capacity of employees and the managementof health or social care systems and services (with a basis in law);
i) the processing is necessary for reasons of public interest in the area of public Health;
j) the processing is necessary for archiving purposes in the public interest, for historical, scientific, research or statistical purposes, subject to appropriate safeguards (with a basis in law)

3.3 Criminal Offence Data

Through the course of its operations, BSWA may be required to process personal data relating to criminal convictions and offences or related security measures. The UK GDPR refers to this as Criminal Offence Data, which includes:

- criminal activity;
- allegations;
- investigations and proceedings.

It may also include personal data about:

- unproven allegations; and
- information relating to the absence of convictions.

It also covers a wide range of related security measures, including

- personal data about penalties;
- conditions or restrictions placed on an individual as part of the criminal justice process; or
- civil measures which may lead to a criminal penalty if not adhered to.

In addition to an Article 6 (above) basis for processing, Criminal Offence Data can only be processed if it is:

- under the control of official authority; or
- authorised by domestic law and meets one of the conditions in Schedule 1 of the DPA 2018.

4. Data Protection Principles

All personal data processed by BSWA must be guided by the six principles set out in the GDPR. BSWA is responsible for and must be able to demonstrate compliance with these principles:

1) Lawful, Fair & Transparent Processing: personal data shall be processed lawfully, fairly and in a transparent manner in relation to individuals;
2) Purpose Limitation: personal data shall be obtained for one or more specified, explicit and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes;
3) Data Minimisation: personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
4) Accuracy: personal data shall be accurate and, where necessary, kept up to date;
5) Retention, Archiving and Removal: personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
6) Security, Integrity and Confidentiality: personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

5. Lawful, Fair & Transparent Processing

All personal data processed by BSWA will be underpinned by an appropriate lawful basis, as set out in the UK GDPR. If BSWA is processing Special Category or Criminal Offence Data, a condition forprocessing this data will be identified and any necessary Data Protection Impact Assessment (15) will be prepared.

BSWA will only handle personal data in a manner in which the data subject would reasonably expect and it will never be used to have an unjustifiable adverse effect on data subjects. Personal data may sometimes be used in a way that negatively affects an individual but only ever if considered, with the advice of the Data Protection Officer (11.1) and only if justified.

BSWA is committed to ensuring that it is clear, open and honest with data subjects regarding the collection, retention and processing of their personal data. This will be provided via appropriate privacy statements, which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a data subject can easily understand what happens to their personal data.

Whenever BSWA collects personal data directly from data subjects, for example for the recruitment and employment of staff and for delivery of support services for women and children, at the time of collection BSWA must provide the data subject with clear information regarding the purpose, storage and use of that data and their rights, as set out in Clause 13. Data Subjects have the right to access their personal data and any such requests (13.1) made to the charity shall be dealt with in a timely manner.

6. Purpose Limitation

BSWA will only collect personal data for specified, explicit and legitimate purposes and it must not be furtherprocessed in any mannerincompatible with those purposes. Where data sharing agreements are in place with partners, this must be made clear to data subjects.

Provided that safeguards are implemented, further processing for scientific or historical research purposes or for statistical purposes will not be regarded as incompatible. For example, BSWA may process information for research purposes but will always anonymise data before doing so.

7. Data Minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. BSWA will not, therefore, amass large volumes of personal data that are not relevant for the purposes for which they are intended to be processed. This includes undue repetition or duplication of personal data in numerous systems across the organisation. BSWA will provide staff with appropriate systems and training to ensure personal data is effectively and securely stored and accessible. However, personal data must be adequate to ensure that BSWA fulfil the purposes for which it was intended to be processed.

BSWA will ensure that when personal data are no longer needed for the specified purposes, they are deleted or anonymised, in accordance with the data retention schedule.

8. Accuracy

BSWA will ensure that all personal data is accurate and, where necessary, kept up to date with adequate and secure systems in place to provide appropriate storage, filing and retrieval.

Incomplete records can lead to inaccurate conclusions being drawn and, where there is such a risk, BSWA staff should ensure that relevant information is complete and accurate, with appropriate responsibilities forreviewing and updating files made clear.

BSWA staff must check the accuracy of any personal data at the point of collection and at regular intervals thereafter, taking all reasonable steps to destroy or amend inaccurate records and updating personal data where necessary.

9. Retention, Archiving & Removal

To guarantee that personal data is kept for no longer than necessary, BSWA shall implement a retention schedule, detailing each area in which personal data is processed, including that which is retained for legal, accounting and reporting purposes, setting out clear retention periods and data removal processes and responsibilities. This process will be reviewed annually by the Information Governance Committee.

The anonymisation and further retention of personal data, beyond the agreed period, along with rationale, will be set out under Archiving in the Data Retention Schedule.

BSWA will take all reasonable steps to destroy or erase from systems all personal data that is no longer required, in accordance with the above retention schedule and in a secure and confidential manner.

Data subjects will be informed of the period for which their personal data are stored and how that period is determined in relevant Privacy Statements.

10. Security, Integrity & Confidentiality

BSWA will commit to providing adequate, secure and modern IT systems that are kept updated and sufficient forthe storage of personal data and the purposes of processing. BSWA will also implement and maintain appropriate safeguards against unauthorised or unlawful processing or accidental loss, destruction of or damage to the personal data that is holds, including providing sufficient training to all staff to ensure all understand their responsibilities under this policy and utilise BSWA systems appropriately and as instructed.

Access to personal data will be limited to personnel under the *principle of least privilege*, ensuring that users are given minimum levels of access – or permissions – needed to perform their specific job functions. For further information regarding IT systems and security, please see BSWAs Internet & IT Policy.

Relevant responsibilities and principles for file restrictions on BSWAs case management system are in place and will be reviewed annually by the Information Governance Committee.

All BSWA staff are responsible for protecting the personal data that they process in the course of their duties. They must, therefore, handle personal data in a way that guards against accidental loss or disclosure or other unintended or unlawful processing and in a way that maintains its confidentiality, ensuring that they are complying with this policy, and related policies, at all times and reporting any concerns regarding the security or confidentiality of personal data to the Data Protection Officer.

Staff must comply with all procedures and technologies BSWA has in place to maintain the security of all personal data from the point of collection to the point of destruction.

11. Accountability

BSWA will implementand maintain appropriate technical and organisational measures to demonstrate its compliance with the UK GDPR, including:

- Adequate training for all staff around the adoption and implementation of this policy and responsibilities
- Ensuring written contracts are in place with organisations that process personal data on its behalf or organisations with which BSWA shared data controller responsibilities
- Maintaining documentation of processing activities
- Implementing appropriate security measures
- Recording and, where necessary, reporting personal data breaches
- Conducting Data Protection Impact Assessments for uses of personal data that are likely to result in high risk to individuals

BSWA has convened an Information Governance Committee, who will take responsibility for developing and monitoring comprehensive, effective and compliant Information Governance Framework at BSWA, reviewing this policy and related procedures annually and collaborating on any required improvement initiatives and in the event of data breach incidents.

11.1 Data Protection Officer

BSWA is registered with the Information Commissioner's Office and has appointed Kathleen Williams **as Data Protection Officer**: kathleen.williams@bswaid.org

11.2 Data Breach

A personal data breach means 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.

The GDPR requires BSWA report to the Information Commissioner's Office (ICO) any personal data breach where there is a risk to the rights and freedoms of the data subject. Where the Personal data breach results in a high risk to the data subject, they must also be notified unless subsequent steps have been taken to ensure that the risk is unlikely to materialise, security measures were applied to render the personal data unintelligible (e.g. encryption) or it would amount to disproportionate effort to inform the data subject directly. In the latter circumstances, a public communication must be made or an equally effective alternative measure must be adopted to inform data subjects, so that they themselves can take any remedial action.

BSWA has procedures in place to manage any suspected personal data breach. If staff know or suspect that a personal data breach has occurred, they should immediately contact the Data Protection Officer and follow their instructions. The DPO will investigate and determine if the breach is reportable to the Information Commissioner's Office and/or data subjects. The DPO will also advise on action that is required internally and provide guidance to assist with mitigating risk of future breaches.

A central process will be maintained to monitor data breach *near misses* and a report provided to the Senior Leadership Team on a quarterly basis, in order to identify and proactively rectify any potential threats to this policy.

Where there is deliberate misconduct or behaviour amounting to a wilful breach of this Data Protection Policy, or gross negligence causing a breach of the policy, the matter may be considered under BSWAs Disciplinary Policy.

12. Transferring Data Outside of the UK

The UK GDPR restricts the transfer of personal data to countries outside the UK or to international organisations unless appropriate safeguards are in place.

A restricted transfer may be made if the receiver is located in a third country or territory or is an international organisation covered by UK adequacy regulations. If adequacy regulations are not met, appropriate safeguards must be in place and documented between both parties.

If data are anonymous so that it is never possible to identify individuals (even when combined with other information which is available to receiver), it is not personal data and the restrictions do not apply. This anonymous data can, then, be transferred outside of the UK.

13. Data Subject Rights

Data protection legislation provides the following rights for data subjects:

1) The right to be informed about the collection and use of their personal data;
2) The right of access to access and receive copies of their personal data;
3) The right to rectification to have inaccurate personal data rectified, completed or updated
4) The right to erasure (or 'to be forgotten') - to ask for personal data to be erased. This is not absolute and safeguarding of vulnerable adults and children will always be considered
5) The right to restrict processing - to request restriction or suppression of their personal data. This only applies in certain circumstances and storage of the data is still permitted;
6) The right to data portability- to obtain and reuse their personal data for their own purposes across different services;
7) The right to object to the processing of their personal data in certain circumstances;
8) Rights in relation to automated decision making and profiling

BSWA has procedures in place for complying with any of the above requests and any queries should be directed to the Data Protection Officer.

13.1 Data Subject Access Requests

Any individual that BSWA holds and processes personal data for can request access to their data in line with the above rights. Requests can be made verbally, by email or by social media and the organisation has one month to respond. BSWA, therefore, has a procedure for responding to Data Subject Access requests, which all staff should be aware of and comply with.

14. Sharing Personal Data

The General Data Protection Regulations (GDPR) and Data Protection Act (DPA) 2018 allow social care organisations and local authorities to share information for a variety of reasons which are known as 'legal bases to process data'. The data protection legislation should never be used as a 'blocker' when sharing personal data, especially in times of emergency which require collaborative working internally and externally.

We will always aim to share the minimum data necessary to achieve the purpose required and, where possible, consent will always be sought.

Substantial public interest

Article 9 (2)(G) of GDPR

BSWA is able to share data, both internally and externally, if it satisfies the Data Protection Act's definition of 'substantial public interest', (Schedule 1, paragraphs 6 - 28). There are 23 specific definitions and those most relevant include using data to:

- Fulfil an explicit statutory or government purpose
- Protect the public
- Satisfy external regulators
- Better provide support for individuals with a particular disability or medical condition
- Safeguard children and individuals at risk, and
- Safeguard the economic well-being of certain individuals

Statutory obligation to share data

Article 9 (2)(B)) of GDPR

GDPR allows BSWA to share data if it is necessary to comply with the obligations set out in law. Local Authorities are given many powers in different Acts of Parliament which can be used in the context of emergency data sharing and these powers may apply to the contractual obligations that BSWA holds to Local Authorities and statutory organisations.

The list below shows some of the most frequently used, but is not exhaustive:

- Care Act (2014), this allows councils to share data to promote individual well-being, prevent the individual need for care and to support and promote the integration of health and social care
- Children's Act (1989), this allows councils to share data to safeguard and promote the wellbeing of children
- Homelessness Reduction Act (2017), this allows councils to share data as part of taking reasonable steps to help applicants secure accommodation

Other specific legal bases covered under GDPR

GDPR also sets out other legal bases for sharing 'special category data' which can be used in specific scenarios. These include when it is:

- necessary for the provision of social care or health care treatment or for the management of a health or social care system. This condition is only met if both sharing parties are 'health and social care professionals using the data to provide direct care to the individual (Article 9 (2)(H) of GDPR)
- in the public interest in the area of public health. There needs to be a wider public benefit to share the data. Examples include responding to pandemics or public health monitoring/statistics (Article 9 (2)(I) of GDPR)

If the need to share data corresponds with one of the Article 9 conditions described above, it is likely that this sharing is justified and is serving a larger purpose in response to an emergency or safeguarding women and children.

14.1 Data Sharing Agreements

Data Sharing Agreements should be discussed with all statutory organisations that BSWA enters into contract with, which will require the processing and sharing of personal data between organisations. Being clear on what data needs to be shared and why we need to share data will help BSWA to establish effective and compliant processing for the purpose set out in the Data Sharing Agreement. Data Sharing Agreements should establish which party is controller or if BSWA and the partner organisation are Joint Controllers.

15. Data Protection Impact Assessments

BSWA is required to complete a Data Protection Impact Assessment (DPIA) for types of processing that are likely to result in a high risk to the rights and freedoms of data subjects.

DPIAs should include consultation with the DPO and other relevant individuals or stakeholders where appropriate and should include:

- A description of the nature, scope, context, and purposes of data processing;
- Assess necessity, proportionality, and compliance measures;
- Identify and assess risks to individuals;
- Identify any additional measures to mitigate those risks

For support and guidance in carrying out a DPIA, please contact the Data Protection Officer

16. Direct Marketing and Fundraising Activities

BSWA only collects and stores information related to donors and supporters in line with GDPR, where direct marketing activities are undertaken and consent has been obtained. An appropriate and secure Customer Relationship Management System is used to store supporter data and contact with donors, supporters or other stakeholders for matters relating to their gifts or their relationship with BSWA is outside the scope of this policy.

BSWA does not share data with third party organisations and where other organisations are capturing data on BSWA's behalf, as part of a fundraising campaign or activity, the nature of data collection and usage is clearly explained at point of capture.

BSWA is registered with the Fundraising regulator and, as such, abides by their code of fundraising practice.

Email

BSWA uses Mailchimp to send bulk marketing emails. Mailchimp's GDPR

guidelines can be found here: https://mailchimp.com/en-gb/gdpr/ Each email contains the option to *opt out* and be forgotten, with internal processes in place to ensure this request is actioned across all systems.

Other Direct Marketing

BSWA does not undertake any direct marketing by telephone, text message or post at this time. Any future plans to do so would only be considered under compliance with this policy and the UK GDPR.

17. Staff Training and Updates

All new BSWA staff receive a session explaining the UK GDPR and this policy as part of their induction process. They are then required to complete an online training module and assessment prior to receiving access to systems containing personal data. This training is mandatory and must be refreshed every two years. Data protection is also discussed in IT Systems training, Cyber Security training and training in the use of BSWA's Case management System. Regular update emails, reminders regarding related procedures and processes are sent by the Senior Systems & Data Officer to the full staff team and all are encouraged to contact the Data Protection Officer with any queries relating to data protection.

18. Reviewing this Policy

This policy will be reviewed annually by the Information Governance Committee with any and all updates communicated to staff.

Version	1.2		
Status	Approved		
Approved by	Board	Date	20/09/2022
Published Date	01/10/2022	Next review date	January 2024
Date of Original Publication	01/07/2022	Revision frequency	Annual
Related Documents	Data Retention and Archiving Internet and IT Policy Hybrid Working Social Media Policy Subject Access Request Procedure Statement		