SAASSBMK DOCUMENT IDENTITY			
Title:	Data Protection GDPR Policy		
Document Ref:		**Version:**	Fourth Version
Date of original publication:	May 2018	**Date of this version:**	November 2025
Review Scheduled:	May 2026	**Obsoletes:**	
Status:	Active	**Comments:**	

Data Policy

Purpose and scope

Sexual Assault and Abuse Support Service Buckinghamshire and Milton Keynes (SAASSBMK) is required to process relevant personal data regarding service users, staff, volunteers, trustees, donors, suppliers and any other people we process information about as part of its operation and shall take all reasonable steps to do so in accordance with this policy.

This Policy applies to all personal data we process regardless of the media on which that data is stored or whether it relates to past or present members, employees, workers, clients or supplier contacts, shareholders, website users or any other data subject.

SAASSBMK is registered with the ICO and is considered a Data Controller in that it determines how personal data is collected, stored, and processed.

Roles and Responsibilities

This policy applies to all staff, volunteers, and external organisations or individuals working on our behalf. Individuals who do not comply with this policy may face disciplinary action.

SAASSBMK's trustees have an overall responsibility for ensuring that the organisation complies with its legal obligations.

SAASSBMK has appointed the CEO as the Data Protection Officer who will endeavor to ensure that all personal data is processed in compliance with this policy and the principles of the Data Protection Act 2018, the UK General Data Protection Regulations (UK GDPR) and any other relevant legislation.

All staff and volunteers are responsible for ensuring personal data is collected, stored, used and kept up to date in compliance with this policy. They are also responsible for ensuring data is safeguarded against unauthorised access, stored securely or destroyed if no longer required. They require permission from the Data Protection Officer to disclose data to a third party outside of already agreed arrangements or change the use of data.

Line managers are responsible for outlining staff and volunteers' responsibilities during their induction. All new staff and volunteers are required to read a copy of this policy and accept any policies and procedures that relate to the personal data they may handle in the course of their work. Infringement of this policy will be regarded as misconduct.

Please contact the CEO with any questions about the operation of this Data Protection Policy or the UK GDPR in general, or if you have any concerns that this Data Protection Policy is not being or has not been followed.

Definitions

SAASSBMK is a Charitable Incorporated Organisation (CIO)

Consent: an agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them. This includes, where applicable, the consent of staff, volunteers, service user, supporters, and donors.

Data controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. SAASSBMK is the Controller of all Personal Data relating to our Company Personnel and Personal Data used in our business for our own commercial purposes.

Data processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

Data Protection Officer (DPO): DPOs assist an organisation to monitor internal compliance, inform and advise on data protection obligations, provide advice regarding Data Protection Impact Assessments and act as a contact point for data subjects and the Information Commissioner's Office (ICO)

Data subject: an individual who is the subject of the personal data

Information Commissioner's Office (ICO): the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals

Personal data: any information that identifies, directly or indirectly, a data subject. Personal data includes information, facts, photos/media, documents, and records about an individual.

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Processing: refers to any action taken in relation to personal data including, but not limited to, collection, adaptation, alteration, recording, storage, retrieval, consultation, use, disclosure, dissemination, combination or deletion, whether by automated means or otherwise

Special categories of data: data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, biometric data (where used for identification purposes), data concerning health, data concerning a person's sex life or sexual orientation

Our data subjects

SAASSBMK collects personal information from different groups of data subjects:

- Job applicants
- Employees
- Freelancers
- Volunteers
- Service users
- Donors
- Trustees
- Building visitors

- Website visitors and social media data subjects
- Attendees of events

Staff and volunteers should familiarise themselves with the various organisational privacy notices, including the general Privacy Notice (on the website) and the Privacy Notice – Employees and Volunteers. These explain how and why we collect personal data.

The principles of data protection

SAASSBMK shall, so far as is reasonably practicable, comply with the data protection principles contained in the UK GDPR.
We are responsible for, and must be able to demonstrate, compliance with the data protection principles. We do this by implementing records, policies and documents to demonstrate that we are compliant, and these are referenced throughout this policy.

SAASSBMK will ensure that all data is:

1. Fairly and lawfully processed in a transparent manner

We identify a lawful basis for all of the data that we process, and document these in our Record of Processing Activity.

We have a comprehensive, publicly available privacy notice to ensure we are transparent with our data subjects about how we process their data, and we have complied with the legislation to ensure our privacy notice contains all of the information that it needs. We provide this privacy notice to all of our data subjects as soon as is reasonably possible.

2. Processed for a lawful purpose

We only collect data for specified and legitimate purposes, and these purposes are recorded in the ROPA and communicated to data subjects in our privacy notice. Data is not further processed in a way that is incompatible with these purposes. The organisation may extend a purpose to cover new processing, as long as the new purpose is compatible with the old.

3. Adequate, relevant, and not excessive

We identify the personal data that we need to be able to meet our purposes, and only process that data and no more, to ensure we are not processing any unnecessary data.

4. Accurate and up to date

SAASSBMK will endeavour to ensure that all personal data held in relation to all data subjects is accurate. We assume that the data we process is accurate at the time

that it is collected. Data subjects will notify the data processor of any changes to information held about them, and we store data in a format that means it's easily rectifiable if we need to update it.

You must update the organisation of any changes to their personal data so that we can keep staff records up-to-date.

5. Not kept for longer than necessary

SAASSBMK will not keep data for longer than it is needed, and anonymises, deletes, destroys or securely disposes of data once its retention date has passed.
Retention times are not stated in data protection legislation, so these are based on legal, regulatory, operational or practical decisions, and are logged in our ROPA.

You must comply with the organisation's guidelines on Data Retention. You will take all reasonable steps to destroy or erase from our systems all Personal Data that we no longer require in accordance with the organisation's records retention schedules. This includes requiring third parties to delete that data where applicable. Should any personal data be required to be retained beyond the retention period, this may only be done with the express written approval of the Data Protection Officer, and must be in line with data protection requirements.

SAASSBMK specifically directs users not to destroy data in violation of this policy. Destroying data that a user may feel is harmful to themselves is particularly forbidden or destroying data to cover up a violation of law or SAASSBMK policy.

If any information retained under this policy is stored in an encrypted format, considerations must be taken for secure storage of the encryption keys. Encryption keys must be retained if the data that the keys decrypt is retained.

SAASSBMK may store some data such as registers, photographs, achievements, books, and documents etc indefinitely in its archive. Where a data subject can be identified, images will be processed as personal data.

6. Secure

SAASSBMK maintains appropriate physical and digital security measures to keep the data it processes secure. The organisation limits access to the data only to those who need such access to provide services to data subjects, or for other legitimate purposes. SAASSBMK and therefore all staff, volunteers and trustees are required to respect the personal data and privacy of others and will ensure that appropriate protection and security measures are taken against unlawful or unauthorised access to processing of personal data, and against the accidental loss of, or damage of, all personal data.

An appropriate level of data security will be deployed for the type of data and the data processing being performed. In most cases, personal data will be stored in appropriate systems and be encrypted when transported offsite. Other personal data may be for publication or limited publication within SAASSBMK, therefore having a lower requirement for data security.

IT and digital security measures
There are several general IT measures that SAASSBMK puts in place to help ensure the security of its data, including (but not limited to):

- Using only authorised software products
- Providing staff with email guidance and training, ensuring they are aware of when to use BCC function
- Using strong passwords
- Using password protection and multi-factor authentication where possible
- Encrypting files where possible
- Regularly updating software
- Using secure wi-fi and avoiding the use of unsecure public wi-fi

Physical security measures
There are also physical security measures that SAASSBMK puts in place, including (but not limited to):

- clear desk policy to avoid people leaving confidential data on their desk
- locked filing cabinets, drawers or lockers for confidential paperwork
- automatic screen shut down when staff members are away from their computer
- arrangements for shredding paper
- shredding and disposing of manual records which have passed their retention as ‘confidential waste’

Attention is also drawn to the existence of the SAASSBMK IT Acceptable Usage Policy which provides more specific information on the use of computers and technology.

MSA Trust operates under a policy of confidentiality. The organisation is committed to providing confidential services to their stakeholders and ensuring that all personal data about staff, trustees, donors, service users and any other stakeholders is treated as confidential and is collected, processed and retained in line with the data protection law. In certain situations, however, information may need to be shared with third parties, for example to protect the welfare and safety of people that are part of the organisation.

When implementing any new systems, processes, services or projects that are likely to involve personal data in any way, a Data Protection Impact Assessment (risk assessment) must be completed to show we have considered the risks and we will do everything to keep the data secure.

7. Not transferred to other counties without adequate protection

Where personal data is stored or transferred outside of the UK and the EU, safeguards to protect personal data may include, but are not limited to, the UK Addendum used in conjunction with the EU Standard Contractual Clauses (SCCs), or UK International Data Transfer Agreement (IDTAs). Such safeguards will be subject to Transfer Risk Assessments (TRAs).

The six lawful bases for processing personal data, and special categories of data

SAASSBMK processes personal data by identifying a 'lawful basis' chosen from the six possibilities set out in the UK GDPR. The most common lawful bases that the organisation identifies are those stated below - consent, contract, legal obligation and legitimate interest. The lawful bases for different processing activities are recorded in the ROPA spreadsheet which is maintained and reviewed regularly.

Consent
If we choose consent as our lawful basis, it means that the data subject has given their consent to the processing of their personal data for one or more specific purposes. The organisation will gather proof of that consent. The data subject has the right to withdraw their consent at any time. Please see the "data subject rights" section of this policy for more information.

Consent to the processing of personal data by the data subject must be:

- Explicit i.e. demonstrated by active communication between the data controller and the data subject and must not be inferred or implied by omission or a lack of response
- Freely given and should never be given under duress, when the data subject is in an unfit state of mind or provided on the basis of misleading or false information
- Specific and informed, it should cover the organisation's name, the purposes of the processing and the types of processing activities
- A clear and unambiguous indication of the wishes of the data subject

The organisation understands that consent is for the time being, and may review and refresh consent as appropriate. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

Contract
The organisation identifies contract as its lawful basis when processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering a contract.

Legal obligation

The organisation identifies legal obligation as a lawful basis when processing is necessary for compliance with a legal obligation to which we are subject.

Legitimate interests
If the organisation has a legitimate interest and processing data is necessary to achieve it, the organisation chooses legitimate interest as its lawful basis. A Legitimate Interest Assessment is completed in order to show what our interest is and that it is legitimate, to show why the processing is necessary in pursuing this interest, to consider potential impact on any data subjects' rights and freedoms and to measure whether the data subject might reasonably expect the organisation to process their data. Data subjects always have a right to object to the processing of their data when legitimate interest is the lawful basis for processing. Please see the "data subject rights" section of this policy for more information.

When processing *special category data* (race/ethinicity, religious/philosophical beliefs, trade union membership, health information, genetic/biometric data, political opinions, sex life/sexual orientation) or criminal record data without the consent of the data subject, data protection law requires us to identify another lawful basis other than consent, supported by a further condition. This might need to be further supported by additional conditions from the Data Protection Act 2018.
The organisation has completed an Appropriate Policy document for the processing of special category data and criminal data without consent of the data subjects as required by law.

Breaches of Data Security

All staff and volunteers are responsible for reporting a loss of data or inadvertent disclosure of data to the Data Protection Officer. The incident should be investigated by the Data Protection Officer or delegated to an appropriate person who has sufficient resources to investigate.

The investigation should include:

- An assessment of risk, including whether the loss is an inconvenience or if sensitive and/or personal data has been lost, any risk of harm to persons as a result of the loss, and any level of security protecting it at the time e.g. encryption.
- Who should be made aware of the breach and any containment measures that can be taken, and if any organisations or authorities such as the ICO, banks or the police should be informed.
- Whether the data can be recovered.

These details should be recorded in the Data Breach Log.

If the breach is likely to adversely affect the personal data or privacy of service users or other users, we need to notify them of the breach without unnecessary delay.

Details about how to do this are on https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/#whendowe

If a data subject has been harmed by a breach of data protection legislation, they can take the controller to court for compensation.

In some cases notification may be required to the Information Commissioners Office within 72 hours, and guidance on this can be obtained at: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breaches-a-guide/#whatbreachesdo

Once the incident has been contained and managed, evaluation should be undertaken to establish how a repeat could be avoided and if any action is required to ensure this. This may include revision of policies or procedures, and/or replacement of equipment. It should also be established if any unclear responsibilities contributed to the incident, and if additional staff training is required.

Data subject rights

SAASSBMK is fully aware of data subject rights, and these are listed in the privacy notice.
The data subjects' rights include:

The right to be informed
Data subjects have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UK GDPR. The organisation is committed to comply with this right and they do so via the privacy notice.

The right of access and Subject Access Requests
A data subject has the right to make access requests in respect of personal data that is held and disclosed about them, known as a Subject Access Request. It is important to know that data subjects can make this request in any format they wish (including verbally) and they do not need to direct their request to a particular member of staff. The Data Protection Officer shall be the person responsible to deal with and respond to SARs. The organisation has one month to respond to an SAR, so it's imperative that staff pass on anything that might be a Subject Access Request to the Data Protection Officer without delay.

The DPO will:

- Ask for 2 forms of identification if we are not satisfied of the identity of the requester;
- Decide whether we need to contact the individual by phone to verify the request;
- Respond within 1 calendar month (or earlier if the deadline falls on a non-working day);

- Extend this by a further 2 months if the request is complex (https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/right-of-access/what-should-we-consider-when-responding-to-a-request/#extend);
- Redact the data so only the requester's data is left, making sure not to leave any personal data of anyone else in unless we have their consent;
- Not disclose information if an exemption applies (guidance here https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/right-of-access/what-other-exemptions-are-there/);
- Provide the information free of charge in a secure way, alongside our privacy notice and information about how they can complain if they're unhappy with the way the SAR has been processed.

As part of our aim to empower survivors, we have always made available to service users their notes and records upon written request. However, reading these notes may be distressing and a request to do so may reflect a testing of the boundaries of their relationship with SAASSBMK. We would speak with a service user about the implications of such a step before they read their notes.

Third-parties may submit SARs on behalf of other individuals, but they must have clear permission from the data subject e.g. written permission or a power of attorney document. If there is no evidence that a third-party is authorised to act on behalf of an individual, the organisation is not required to comply with the SAR, however we should still respond to them explaining this.

When it comes to requests for the data of children, a decision will be made on a case-by-case basis. A parent/carer does not have automatic rights to view a child's data, and we should get consent from children before releasing their data to a third party.

All SARs will be logged internally.

The right of rectification
If the data subject becomes aware that the organisation is holding incorrect information about them, they have the right for it to be corrected, and if their information is incomplete, they can also submit additional information to be added.

The right to erasure/be forgotten
If a data subject asks the organisation to delete their information the organisation will do so when:

- the personal data is no longer necessary in relation to the purposes for which it was collected or otherwise processed
- the data subject withdraws consent (if that is the basis on which the processing is taking place), and where there is no other legal ground for the processing
- the data subject objects to the processing and there are no overriding legitimate grounds for the processing

- the personal data has been unlawfully processed
- the personal data has to be erased for compliance with a legal obligation or
- the personal data has been collected in relation to the offer of online services to a child

In addition, if the organisation has made the information public, we must try to have it erased in other locations as well. We must also inform any third parties to whom the data subject's data has been disclosed, unless this 'proves impossible or involves disproportionate effort'. The organisation will also inform the data subject which recipients their data has been disclosed to, if they ask.

There are exceptions to the 'right to be forgotten' for reasons relating to freedom of expression, public health, archiving, research and statistics, legal claims and legal obligation.

There may also be circumstances where the organisation has no choice but to retain data, for example to mark a record for suppression to ensure that no direct marketing is sent to that individual in the future.

The organisation will process a request for erasure without undue delay, and within one month of receipt.

The right to restrict processing
The data subject shall have the right to restriction of processing of their personal data where one of the following applies:

- the accuracy of the personal data is contested by the data subject, for a period enabling us to verify the accuracy of the personal data
- the processing is unlawful, and the data subject opposes the erasure of the personal data, requesting the restriction of its use instead
- we no longer need the personal data for the purposes of the processing, but it is required by the data subject for the establishment, exercise or defence of legal claims
- the data subject has objected to processing pending the verification whether the legitimate grounds of SAASSBMK override those of the data subject

The right to data portability
This right applies when processing is based on consent or a contract between the organisation and the data subject, and the processing is taking place 'by automated means'. It allows data subjects to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.

Data subjects are entitled to receive from the organisation a copy of any personal data they have provided in a 'structured, commonly used and machine-readable format', so that they can provide the data to a different organisation.

The right to object

Data subjects can object to any processing of their data that organisation is carrying out on the lawful basis of legitimate interests. The organisation will stop processing if not able to demonstrate 'compelling legitimate grounds'.

Rights in relation to automated decision making and profiling
The data subject has the right to object to profiling and a right to be informed of the fact that profiling is taking place, as well as the intended outcome(s) of the profiling. The data subject has the right not to have decisions made about them solely by automated processing if this has a significant effect on them, unless the decision is necessary in conjunction with a contract between the data subject and the organisation, or the data subject has provided explicit consent.

The right not to receive direct marketing
Every data subject has the right not to receive direct marketing if that is their choice. If an individual opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

The right to claim damages in case of a data breach
If a data subject has been harmed by a breach of data protection legislation, they can take the controller to court for compensation.

The right to complain
If data subjects wish to make a complaint or share concerns, they should be firstly encouraged to liaise directly with the organisation. They can make a complaint to the service lead or email ceo@saassbmk.org.uk who will respond promptly.

Data subjects are informed via the privacy notice that they can also make a complaint to the ICO.

All staff members should be aware of how to recognise an incoming request to exercise any right, to understand when the right applies and to pass it on without delay to the designated person. Under certain circumstances, the organisation may not need to comply with the request by a data subject to exercise one of their rights. Those circumstances will be assessed on a case-by-case basis.

Working with, and sharing data with, other organisations

As with any other organisation, SAASSBMK may collaborate with:

- data processors (a company, organisation or individual who is not an employee or volunteer, that processes data on behalf of SAASSBMK)
- joint data controllers (where two or more data controllers jointly determine the purpose and means of processing)
- separate data controllers (another organisation which is a separate controller, and information is merely disclosed to one other).

All third parties we work with who have or may have access to personal data of our data subjects will either comply with this policy, or we will ensure that their data protection policy aligns with this policy.

We put in place Data processor Agreements, Data Sharing Agreements or Joint Controller Agreements before sharing personal data with other organisations.

Enforcement

If an individual believes that SAASSBMK has not complied with this policy or acted otherwise than in accordance with the UK GDPR or Data Protection Act, the individual should utilise the SAASSBMK grievance procedure in cases of employees or the complaints procedure in cases of service users and volunteers. You also have the right to notify the Information Commissioners Office (ICO).

Duty of Candour

We will ensure candour by being open and honest about anything going wrong and promptly inform our service users of anything in our work that places service users at risk of harm, or has caused them harm, whether or not the service user(s) affected are aware of what has occurred by:

a. taking immediate action to prevent or limit any harm
b. repairing any harm caused, so far as possible
c. offering an apology when this is appropriate
d. notifying and discussing with our supervisor and/or manager what has occurred
e. investigating and take action to avoid whatever has gone wrong being repeated

SAASSBMK may store some data such as registers, photographs, achievements, books, and documents etc indefinitely in its archive. Where a data subject can be identified, images will be processed as personal data.

Retention requirement

This section sets guidelines for retaining the different types of SAASSBMK data.

Personal client data	six years from end of service user being involved with SAASSBMK
Personal employee data	six years from end of employment
Tax payments	six years

Records of leave	three years
Recruitment details	interview notes of unsuccessful applicants kept for one year. CV's and application forms kept for six months.
Planning data	seven years
Health and Safety	seven years for records of major accidents and dangerous occurrences
Public data	three years
Operational data	five years. Most SAASSBMK data will fall into this category.
Critical data including tax and VAT	six years
Confidential data	seven years

Due to the nature and importance of protecting the data of all individuals involved with SAASSBMK, this policy will be reviewed annually.