****

**Shetland Women’s Aid**

**Data Protection Policy**

**1. Policy Statement**

Shetland Women’s Aid Women’s Aid (SWA) delivers services to women, children and young people who are experiencing domestic abuse. Shetland Women’s Aid are committed to being transparent about how it collects and uses the personal data of its workforce, and to meeting its data protection obligations. This policy sets out the SWA's commitment to data protection, and individual rights and obligations in relation to personal data.

SWA needs to process certain information about its employees, clients, and other individuals it has dealings with for a range of purposes (for example, to recruit and pay employees, to record progress and training) and to comply with contractual and legal obligations.  Clients and employees have the right to confidentiality and therefore information that identifies individuals should be shared only when there are clear and valid reasons for doing so.  Whether personal information is collected and used on paper or electronically, it must be processed in accordance with the law.

SWAmay also process personal information (and data relating to criminal offence(s)) about perpetrators and alleged perpetrators. The organisation is permitted to do this under several exemptions contained in the Data Protection Act 2018 and relevant Schedules. This information will be treated in the same way as other personal data and sensitive personal data, for example, we will use the appropriate technical and organisational measures to keep this information secure and to protect it against unauthorised or unlawful processing and against accidental loss destruction or damage.

SWAtakes the security and privacy of personal information seriously. The organisation gathers and uses data about you in the normal course of their business and the delivery of their services and to manage their relationship with you and others with whom they have dealings and come into contact.

SWA may also have to share information about individuals and will aim to do this in line with this policy, privacy notices and information-sharing protocols.

SWA is required to comply with the law governing the management and storage of personal data, which is set out in the Data Protection Act 2018 and the General Data Protection Regulation 2016 (GDPR).

# Policy Aims

This policy aims to protect and promote the data protection rights of individuals and of the business by informing everyone working for the business of their data protection obligations and of the business procedures that must be followed to ensure compliance with the GDPR.

Its purpose is also to ensure that our employees and volunteers understand and comply with the rules governing the collection, use and deletion (all of which is known as ‘processing’) of personal information to which they may have access in the course of their work.

We are committed to complying with our data protection obligations and to being concise, clear, and transparent about how we obtain, use, and share personal information relating to our workforce, volunteers, service users and others and how and when we delete that information once it is no longer required.

We have several privacy statements that can be found in the Data Protection folder in our shared drive library called Office.

Our retention policy/schedule will give you information about how we dispose of (destroy) records and data retention.

# Scope

This policy applies to the personal information of job applicants, current and former staff, including employees, temporary and agency workers, volunteers, casual or contract staff, suppliers, service users, partners, funders and any other third party we have dealings with.

We will review and update this policy in accordance with our data protection obligations. It does not form part of any employee’s contract of employment, and we may amend, update or supplement it from time to time. We will circulate any new or modified policy to staff and relevant others before it is adopted.

# Responsibilities

4.1 SWAis responsible for ensuring:

* that our employees and volunteers are aware of this policy
* that they receive the appropriate level of training to support the implementation of this policy
* the Information Commissioner entry is up-to-date and accurate.
* that data is processed in line with SWApolicies and procedures.
* that this policy is implemented and enforced
* that any suspicious activities are reported
* all subject access requests are managed appropriately.

4.2 All employees, trustees and volunteers have responsibilities to comply with the data protection principles outlined in section 5 below. They should:

• not disclose any personal information outside the organisation’s procedures nor use it for their purposes. Anyone disclosing information without the authority of the organisation may commit a criminal offence and may also be subject to disciplinary proceedings.

* ensure that they are familiar with, and comply with, the terms of this policy.
* ensure that they provideSWAwith relevant and accurate personal data about themselves.

# Data Protection Principles

SWAwill comply with the following data protection principles when processing personal information and will comply with these in the following ways:

* we will process personal information lawfully, fairly and in a transparent manner.
* we will collect personal information for specified, explicit and legitimate purposes only, and will not process it in a way that is incompatible with those legitimate purposes.
* we will only process the personal information that is adequate, relevant, and necessary for the relevant purposes.
* we will keep accurate and up-to-date personal information and take reasonable steps to ensure that inaccurate personal information is deleted or corrected without delay.
* we will keep personal information,in a form which permits the identification of data subjects**,** for no longer than is necessary for the purposes for which the information is processed.
* we will take appropriate technical and organisational measures to ensure that personal information is kept secure and protected against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

# Individual Rights

You have the following rights about your personal information:

* to be informed about how why and on what basis that information is processed.
* to obtain confirmation that your information is being processed and to obtain access to it and certain other information by making a subject access request.
* to have data corrected if it is inaccurate or incomplete.
* to have data erased if it is no longer necessary for the purpose for which it was originally collected/processed or if there are no overriding legitimate grounds for the processing (known as the right to be forgotten)
* to restrict the processing of personal information where the accuracy of the information is contested, or the processing is unlawful (but you do not want the data to be erased), or where the organisation no longer needs the personal information, but you require the data to establish, exercise or defend a legal claim.
* to restrict the processing of personal information temporarily where you do not think it is accurate (and the employee is verifying whether it is accurate) or, where you have objected to the processing (and the organisation is considering whether their legitimate grounds override your interests.)

Should you wish to exercise any of these rights, or for more information please contact the Manager in the first instance.

# Individual Obligations

Individuals are responsible for helping the organisation keep their personal information up to date. You should let your manager know if the information you have provided to the organisation changes, for example, if you move house or change details of the bank or building society account to which you are paid.

Where you have access to the personal information of other members of our workforce, volunteers, service users, suppliers, funders, or partners in the course of your employment or arrangements with the organisation, the organisation expects you to help meet its data protection obligations to those individuals. For example, you should be aware that they may also enjoy the rights set out in paragraph 6 above.

If you have access to others’ personal information, you must:

* only access the personal information that you have authority to access and only for authorised purposes.
* only allow other staff from the organisation to access personal information if they have appropriate authorisation.
* only allow individuals who are not staff from the organisation to access personal information if you have specific authority to do so fromthe Manager.
* keep personal information secure (e.g. by complying with rules on access to premises, computer access, password protection and secure file storage and destruction)
* Do not remove personal information, or devices, containing personal information (or which can be used to access it) from the organisation’s premises unless appropriate security measures are in place (such as encryption or password protection) to secure the information on the device.
* Do not store personal information on local drives or on personal devices that are used for work purposes.

You should contact the Manager if you are concerned or suspect that one of the following has taken place (or is likely to take place).

* processing of personal data without a lawful basis for its processing or, in the case of sensitive personal information, without one of the additional conditions for processing being met.
* any data breach including those set out in paragraph 12 below.
* access to personal information without the proper authorisation
* personal information not kept or deleted securely.
* removal of personal information, or devices containing personal information (or which can be used to access it) from the organisation’s premises without appropriate security measures being in place.
* any other breach of this Policy or any of the data protection principles set out in paragraph 5.

# Data Security

The organisation will use appropriate technical and organisational measures to keep personal information secure and to protect against unauthorised or unlawful processing and against accidental loss, destruction or damage.

**8.1** SWA **will** ensure that the personal data they hold will be secure and safe from unauthorised or inadvertent alteration or erasure and that access and disclosure will be properly controlled. SWAwill ensure that appropriate security measures are implemented.

**8.2** All personal information in the form of physical records will be kept in a locked filing cabinet, drawer or other secure area with access limited to those who have the right or a need to access it.

**8.3** All personal information in the form of computerised records will be password protected, kept on a secure IT system, and kept only on a secure storage device. This includes tablets, laptops, desktops, and mobile phones.

**8.4 Personal** and sensitive personal information that is no longer required will be deleted permanently from the organisation’s information systems and any hard copies will be destroyed securely.

# Confidentiality

SWA confidentiality policy sets out the limits of confidentiality about data held about service users by SWA**.**

SWA also has a duty of confidentiality in terms of records kept about our employees, volunteers, and others and will inform them about the data kept and how this will be used and shared through privacy notices.

# Management of Records

SWAwill:

* ensure that adequate records are maintained to account fully and transparently for all actions and decisions to ensure that legal and other rights of those affected are protected.
* identify what records they are required to hold and how these will be used.
* develop appropriate systems for collecting, maintaining using, and storing (i.e. processing) this information.
* ensure as far as possible that all records are complete and accurate the information, they contain is reliable and its authenticity can be assured
* ensure that records and the information within them can be efficiently retrieved by those with a legitimate right of access, for as long as the records are held by the organisation.

# References

The provision of an employment reference will generally involve the disclosure of personal data.

**Any reference must be fair and accurate, and its contents must be approved by the appropriate manager/worker with management responsibility before being sent. References should avoid giving objective opinions or comments that are not supported by facts.**

**A personal reference may be given by a member of staff in an individual capacity only. Such a reference must make clear that it is not given on behalf of SWA and must not be provided on SWA-headed paper.**

Under the Data Protection Act 2018, an employee of SWAhas no automatic entitlement to see the contents of a reference provided by a previous employer. Nor is there any obligation on SWAto disclose a reference being provided for an existing employee to a potential future employer.

# Non-Compliance and Data Breaches

Any non-compliance by staff with this policy will normally be dealt with through the SWADisciplinary Policy.

Any non-compliance by volunteers with this policy will normally be the same as for staff and trustees.

A data breach may take many different forms, for example:

* loss or theft of data or equipment on which personal information is stored.
* unauthorised access to or use of personal information either by a member of the workforce or third party.
* human error such as accidental deletion or alteration of data.
* deliberate attacks on IT systems such as hacking, viruses phishing scams.
* unforeseen circumstances such as a fire or flood.

SWA will make the required report of a data breach to the Information Commissioner’s Office without undue delay and where possible and appropriate, within 72 hours of becoming aware of it, if it is likely to result in a risk to the rights and freedoms of individuals and notify the affected individuals if a data breach is likely to result in a high risk to their rights and freedoms and notification is required by law.

# Privacy Statements & Consent Forms

In line with the Data Protection legislation, SWAhas created a set of privacy statements and consent forms for employees, job applicants, funders, women, children, and young people**.** These can be found in our shared drive library named Office under Data Protection.

The information provided in our privacy statements and consent forms is provided in a concise, transparent, intelligible, and easily accessible format using clear and plain language.

# Subject Access

Individuals have the right to access their personal data; this can be requested verbally or in writing. SWA will normally respond to a request no later than one month after receiving it.

We may extend the response time by up to a further two months if the request is complex or if we have received several requests from the individual; we will let the individual know within one month of receiving their request and explain why the extension is necessary.

We will not charge a fee to respond to the initial requests in most circumstances. However, if the case is complex or if we have to provide a lot of information, we may charge for administration costs.

Sometimes we might ask individuals to confirm their identity; we will only do this if it is necessary.

We will refuse any request that is not about your personal data or if it is manifestly unfounded or excessive, considering whether the request is repetitive.

All requests will be kept securely by SWA until the matter is resolved.

# Complaints

If a service user has a complaint about data protection or the processing of personal or sensitive personal information, you can contact the Manager at office@shetlandwa.org**.**

If you are unhappy with our response, you can contact the ICO at <https://ico.org.uk/make-a-complaint/> or telephone: 0303 123 1113 for further information about your rights and how to make a formal complaint.

If an employee has a complaint about data protection, they should consult our Grievance policy.

# Information and Training

SWA will make available to all employees a copy of the Data Protection policy in a centralised and easily accessible location or a shared file electronically. Training will be delivered and available to ensure that all employees understand the policy and procedure, including the statutory requirements.

# Monitor and Review

SWA will monitor and review this policy at approximately *three yearly intervals* and/or when there are relevant changes in legislation or circumstances.

The Manager is responsible for implementing and monitoring compliance with this policy.

# Data Retention

SWA shall not keep personal data for any longer than is necessary in light of the purpose or purposes for which that personal data was originally collected, held, and processed and in accordance with legislative and statutory requirements.

When personal data is no longer required, all reasonable steps will be taken to erase or otherwise dispose of it without delay.

There are statutory retention periods that are required by law, when retaining employee’s HR records-

* Under the National Minimum Wage Regulations 2015, SWA are required by law to keep records for a period of 3 years after the end of the pay reference period following the one that the records cover, where these must be sufficient to establish that you’re remunerating a worker at a rate at least equal to the national minimum wage.
* Under the Statutory [Maternity Pay](https://www.davidsonmorris.com/maternity-rights-at-work/) (General) Regulations 1986, SWA are required by law to keep statutory maternity pay records for a period of 3 years after the end of the tax year in which the maternity pay period ends, including the medical certificate (Mat B1), together with records of leave dates and pay.
* Under the Statutory [Paternity Pay](https://www.davidsonmorris.com/paternity-rights-at-work/) and Statutory Adoption Pay (Administration) Regulations 2002, SWA are required by law to keep statutory paternity and adoption pay records for a period of 3 years after the end of the tax year in which the pay period ends.
* Under the Statutory Sick Pay (General) Regulations 1982, SWA are required by law to keep statutory sick pay (SSP) records for at least 3 years after the end of the tax year to which they relate, including records of dates of an employee’s period of incapacity for work and records of all payments of SSP SWA made during that period.
* Under the Income Tax (Employments) Regulations 1993, SWA are required by law to keep pay-related records for income tax and national insurance purposes for not less than 3 years after the end of the financial year to which they relate.
* Under the Working Time Regulations 1998, SWA are required by law to keep working time records for a period of 2 years from the date on which the records were made that are adequate to show, where applicable, the maximum weekly limits are being complied with.
* Under the Prevention of Illegal Working regime, right to work documents must be retained and stored securely for the duration of the individual’s employment and for a further two years after they have left the organisation.
* Under the Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 2013 (RIDDOR), SWA are required by law to keep for at least 3 years from the date on which they were made any reports of serious workplace accidents, the diagnosis of occupational diseases and incidents of specified dangerous occurrences.
* Information relating to recruitment for unsuccessful applicants will be kept for 12 months from the interview date. To aid in the management of the recruitment process, Shearwater may keep, indefinitely, a record of the names of applicant who have been shortlisted and/or interviewed.

**Staff/Personnel**

In general, electronic and/or manual staff records are kept for 6 years. The information retained would usually include name and address, positions held and leaving salary.

**Training Records**

We do not hold training records/certificates following termination of employment.

**Disposal of Records**

All personal data must be disposed of in a way that protects the rights and privacy of the data subjects (e.g. by way of shredding, disposal of confidential waste or secure electronic deletion).

|  |  |
| --- | --- |
| Definitions **Personal information** | Sometimes known as personal data.  Information relating to an individual who can be identified (directly or indirectly) from that information.  This can be as simple as a name or a number or could include other identifiers such as an IP address a cookie identifier, or other factors. |
| **Data subject** | The individual to whom the personal information relates. |
| **Data controller** | Gathers and processes (uses) certain information about individuals. (SWA is a data controller)  Responsible for updating data protection registrations. |
| **Data Processor** | Processes data on behalf of the Data Controller (SWA may also be a data processor) |
| **Processing information** | This means obtaining, recording, organising, storing, amending, retrieving, disclosing and/or destroying information, or using or doing anything with it; |
| **Criminal records information** | Personal information relating to criminal convictions and offences, allegations, proceedings, and related security measures; |
| **Data breach** | Means a breach of security leading to the accidental or unlawful destruction, loss, alteration, or unauthorised disclosure of, or access to, personal information. |
|  |  |
| **Sensitive personal information** | Sometimes known as ‘special categories of personal data’ or ‘sensitive personal data’.  This is personal information about an individual’s race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership (or non-membership), genetics information, biometric information (where used to identify an individual) and information concerning an individual’s health, sex life or sex orientation. |
| **Pseudonymised** | The process by which personal information is processed in such a way that it cannot be used to identify an individual without the use of additional information, which is kept separately and subject to technical and organisational measures to ensure that the personal information cannot be attributed to an identifiable individual. |