



THE WOMEN'S CENTRE  
Supporting women in Stockport

Policy Name	Data Protection Policy
Policy Number	18
Date of issue	December 2022
Policy author(s)	Board of Trustees
Officer responsible	Centre Manager
Who policy applies to	All staff employed by the Centre and Volunteers, including Trustees
Relevant policies to be read in conjunction with	Safeguarding Children's Policy Safeguarding Adults at Risk
Date approved	30 <sup>th</sup> November 2022

Date of review	May 2026

**CONTENTS**

1 Introduction..... 3  
Document Scope.....3  
Objectives.....3  
2 General Information.....3  
3 Data retention and processing.....5  
4 Responsibilities of staff.....7  
5 Data Security.....8  
6 Data Protection Impact Assessment (DPIA).....9  
7 Subject Consents.....10  
8 Data Protection Lead.....11  
Appendix 1 – Guidance for the retention of personal data.....12  
Appendix 2 – Legal basis for processing data.....18  
Appendix 3 - Privacy notice for Employees, Workers and Contractors.....20  
Appendix 4 - Privacy notice for Service Users ... .. 29  
Appendix 5- Subject Access Process 30

-

# 1 Introduction

## Document Scope

1.1 The General Data Protection Regulation (GDPR) forms part of the data protection regime in the UK, together with the Data Protection Act, 1998 and regulates the processing of information relating to individuals, this includes the obtaining, holding, using or disclosing of such information, and covers computerised records as well as manual filing systems and card indexes.

Stockport Women's Centre (SWC) will hold the minimum personal information necessary to enable it to perform its functions. All such information is confidential and needs to be treated with care, to comply with the law.

## Objectives

1.2 Data users must comply with the data protection principles of good practice which underpin the GDPR

## 2 General Information

2.1 Stockport Women's Centre must adhere to the general principles of the GDPR, and all staff who process or use personal data must ensure that they abide by these principles at all times. This policy has been developed to ensure this happens. The GDPR principles are that data is:

- a) processed lawfully, fairly and in a transparent manner in relation to individuals;
- b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
- c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
- e) 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

- f) 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.

### 3 Data retention and processing

3.1 Staff must notify the Data Protection Lead (the centre manager of SWC) of any filing system or computer database that contains (or will contain) personal data (e.g. name and address) and complete the relevant notification forms to register the system. This notification will then be added to the organisation's registration that is held by the Information Commissioner for approval.

3.2 This retention and disposal policy is based on best advice from Stockport MBC and must be followed. The data retention policy is attached at Appendix 1 and covers staff and volunteers as well as individuals who access the SWC services.

3.3 Service users, staff and volunteers have the right to access their records which SWC holds. A request can be submitted in writing or verbally. A response will usually be made within 14 working days; exceptionally a response may take up to one month. The subject access process is attached at Appendix 5

3.4 Employees, volunteers, and service users can ask that their records be deleted. The request should be made in writing, if possible, to the Data Protection Lead. If the request is made verbally to the Data Protection Lead they will make a written record of that request on that same day. Requests will normally be dealt with within 14 working days but could, exceptionally, take one month to deal with.

The Data Protection Lead will normally grant a request to delete personal data if:

- the personal data is no longer necessary for the purpose for which it was originally collected or processed;
- SWC is relying on consent as the lawful basis for holding the data, and the individual withdraws their consent;
- SWC is relying on legitimate interests as the basis for processing, and there is no overriding legitimate interest to continue this processing;
- SWC is processing the personal data for direct marketing purposes and the individual objects to that processing;
- SWC has processed the personal data unlawfully; or
- SWC has to do it to comply with a legal obligation.

The request will *not* be granted if the processing is necessary for the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation;
- for the performance of a task carried out in the public interest or in the exercise of official authority;
- for archiving purposes in the public interest, scientific research, historical research or statistical purposes where erasure is likely to render impossible or seriously impair the achievement of that processing; or
- for the establishment, exercise or defence of legal claims.

3.5 SWC has considered the legal basis for processing data. The basis varies for service users, employees and volunteers. The details of the legal basis can be found in Appendix 2.

3.6 SWC has agreed a Privacy Notice for services users and Privacy Notice for employees, workers and contractors. These are easily accessible in the office and available for all people accessing our services.

## **4 Responsibilities of staff**

4.1 It is the responsibility of the Data Protection Lead to:

- assess the understanding of the obligations of SWC under GDPR;
- be aware of our current compliance status,
- identify and monitor problem areas and risks and recommend solutions;
- And promote clear and effective procedures and offer guidance to staff on data protection issues. It is anticipated that this will include familiarisation with GDPR, starting in the new starters induction process, and through training programmes/seminars, annual appraisals and intranet/internet resources.

4.2 It is NOT the responsibility of the Data Protection Lead to apply the provisions of GDPR. This is the responsibility of the individual collectors, keepers and users of personal data. Therefore staff are required to be aware of the provisions of the GDPR, such as keeping records up to date and accurate, and its impact on the work they undertake on behalf of the organisation.

4.3 It is the responsibility of the Service Managers that all computer and manual systems within their respective service areas that contain personal data must be identified and the Data Protection Lead informed for notification purposes.

4.4 Any breach of the Data Protection Policy, whether deliberate or through negligence, may lead to disciplinary action being taken or even a criminal prosecution.

## **5 Data Security**

5.1 All staff are responsible for ensuring that:

- any personal data they hold, whether in electronic or paper format, is kept securely; and
- personal information is not disclosed deliberately or accidentally either orally or in writing to any unauthorised third party.

## **6 Data Protection Impact Assessment (DPIA)**

SWC will undertake a DPIA when any new project requiring processing of personal information is undertaken or when new technologies are introduced on which to store and process data. In undertaking the DPIA SWC will assess:

- the nature, scope, context and purposes of the processing;
- the necessity, proportionality and compliance measures;
- the risks to individuals; and
- additional measures to mitigate those risks.

The Data Protection Lead will have the responsibility of undertaking the DPIA.

Any additional risks in processing or retaining data identified as part of the DPIA will be added to the SWC risk register.

## **7 Subject Consents**

The need to process data for normal purposes will be communicated to all staff, volunteers and service users through the privacy notices. In some cases, if the data is sensitive, for example information on health, race or gender, express consent to process the data must be obtained. This processing may be necessary to operate Stockport Women's Centre's policies such as Health and Safety and Equal Opportunities.

## **8 Data Protection Lead**

8.1 SWC is the data controller as defined in GDPR and is therefore ultimately responsible for implementation.

However, day to day matters, the registration of systems and subject access requests will be dealt with by the Data Protection Lead.

**Signed:** \_\_\_\_\_

**Date:** \_\_\_\_\_

**Kay Day**

**Chair**

**Stockport Women's Centre Board of Trustees**

## Appendix 1 – Guidance for the retention of personal data

This guidance contains recommendations on the retention of personal data (including financial data) in respect of three groups – service users, volunteers and unsuccessful applicants and recommendations on the retention of personal data (including financial data) in respect of staff employment records: retention and erasure guidelines

<b>Group</b>	<b>Length of time for retention</b>
Prospective service users, prospective volunteers and unsuccessful applicants	6 months
Current employees, service users and volunteers	Retained as long as they continue to be service users, employees and volunteers
Past service users	Information retained for 8 years after the end of SWC support or their death
Past volunteers	1 year from the end of volunteering

## **ABOUT THESE GUIDELINES**

These guidelines support Stockport Women's Centre's Privacy Policy and adopt its definitions.

The guidelines are intended to ensure that Stockport Women's Centre processes personal data in the form of employment records in accordance with the personal data protection principles, in particular that:

- Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes.
- Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. When personal data is no longer needed for specified purposes, it is deleted or anonymised as provided by these guidelines.
- Personal data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.
- Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.
- Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage.

Any questions about the operation of the guidelines should be submitted to the Centre Manager of Stockport Women's Centre ("the Manager").

## **LOCATION OF EMPLOYMENT RECORDS**

The Manager holds employment records and can be contacted with any enquiries relating to your personal data.

## **KEEPING INFORMATION UP TO DATE**

Stockport Women's Centre needs to ensure that your personal details are up to date and accurate.

When you first start working for Stockport Women's Centre we record your name, address, next of kin and contact telephone details. In the event that any of these change you should inform the Manager. You will be invited to review and update personal information on a regular basis.

These provisions are intended to complement the data subject rights referred to in the Privacy Policy.

## **GENERAL PRINCIPLES ON RETENTION AND ERASURE**

Stockport Women's Centre's approach to retaining employment records is to ensure that it complies with the data protection principles referred to in these guidelines and, in particular, to ensure that:

- Employment records are regularly reviewed to ensure that they remain adequate, relevant and limited to what is necessary to facilitate you working for Stockport Women's Centre.
- Employment records are kept secure and are protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. Where appropriate Stockport Women's Centre uses anonymization to prevent identification of individuals.
- When records are destroyed, whether held as paper records or in electronic format, Stockport Women's Centre will ensure that they are safely and permanently erased.

## **RETENTION AND ERASURE OF RECRUITMENT DOCUMENTS**

Stockport Women's Centre retains personal information following recruitment exercises to demonstrate, if required, that candidates have not been discriminated against on prohibited grounds and that recruitment exercises are conducted in a fair and transparent way.

Stockport Women's Centre expects to keep candidates' personal information once a recruitment decision has been communicated to them. This is likely to be for six months from the communication of the outcome of the recruitment exercise which takes account of both the time limit to bring claims and for claims to be received by Stockport Women's Centre.

Information relating to successful candidates will be transferred to their employment record with Stockport Women's Centre. This will be limited to that information necessary for the working relationship and, where applicable, that required by law.

Following a recruitment exercise information, in both paper and electronic form, will be held by the Manager. Destruction of that information will take place in accordance with these guidelines.

## **RETENTION AND ERASURE OF EMPLOYMENT RECORDS**

Stockport Women's Centre has regard to recommended retention periods for particular employment records set out in legislation, referred to in the table below. However, it also has regard to legal risk and may keep records for up to seven years (and in some instances longer) after your employment or work with us has ended.

<b>Type of employment record</b>	<b>Retention period</b>
----------------------------------	-------------------------

<p>Recruitment records</p> <p>These may include:</p> <p>Completed online application forms or CVs.</p> <p>Equal opportunities monitoring forms.</p> <p>Assessment exercises or tests.</p> <p>Notes from interviews and short-listing exercises.</p> <p>Pre-employment verification of details provided by the successful candidate. For example, checking qualifications and taking up references. (These may be transferred to a successful candidate's employment file.)</p> <p>Criminal records checks. (These may be transferred to a successful candidate's employment file if they are relevant to the ongoing relationship.)</p>	<p>Six months after notifying candidates of the outcome of the recruitment exercise.</p>
<p><b>Immigration checks</b></p>	<p>Three years after the termination of employment.</p>
<p><b>Contracts</b></p>	
<p>These may include:</p> <p>Written particulars of employment.</p> <p>Contracts of employment or other contracts.</p> <p>Documented changes to terms and conditions.</p>	<p>While employment continues and for seven years after the contract ends.</p>
<p><b>Payroll and wage records</b></p>	
<p>Payroll and wage records</p> <p>Details on overtime.</p> <p>Bonuses.</p> <p>Expenses.</p> <p>Benefits in kind.</p>	<p>These must be kept for at least three years after the end of the tax year to which they relate. However, given their potential relevance to pay disputes they will be retained for seven years after employment ends.</p>
<p>Current bank details</p>	<p>Bank details will be deleted as soon after the end of employment as possible once final payments have been made</p>

PAYE records	These must be kept for at least three years after the end of the tax year to which they relate. However, given their potential relevance to pay disputes they will be retained for seven years after employment ends.
Payroll and wage records	These must be kept for six years from the financial year-end in which payments were made. However, given their potential relevance to pay disputes they will be retained for seven years after employment ends.
Records in relation to hours worked and payments made to workers	These must be kept for three years beginning with the day on which the pay reference period immediately following that to which they relate ends. However, given their potential relevance to pay disputes they will be retained for seven years after the working relationship ends.
Travel and subsistence.	While employment continues and for seven years after employment ends.
Record of advances for season tickets and loans to employees	While employment continues and for seven years after employment ends.
<b>Personnel records</b>	
<p>These include:</p> <p>Qualifications/references.</p> <p>Consents for the processing of special categories of personal data.</p> <p>Annual leave records.</p> <p>Annual assessment reports.</p> <p>Disciplinary procedures.</p> <p>Grievance procedures.</p>	While employment continues and for seven years after employment ends.

Death benefit nomination and revocation forms. Resignation, termination and retirement.	
<b>Maternity records</b>	
These include: Maternity payments. Dates of maternity leave. Period without maternity payment. Maternity certificates showing the expected week of confinement.	Four years after the end of the tax year in which the maternity pay period ends.
<b>Accident records</b>	
These are created regarding any reportable accident, death or injury in connection with work.	For at least four years from the date the report was made.

## Appendix 2 – Legal basis for processing data Valid Lawful Basis under GDPR

<i>Data subject class</i>	<i>Data subject type</i>	<i>Valid lawful basis</i>	<i>Comments</i>
Employer			
	Employees	Contract	By signing the Employment Contract
	Trustees	Consent	
	Volunteers	Contract	By signing the Volunteer Agreement
	Members	Legitimate interests	
Provider of services			
	Service users	Consent	By signing the consent form
Fundraising			
	Donors	Legitimate interests	
	Supporters	Legitimate interests	

### Legitimate Interests Assessment (LIA) under GDPR

	<i>legitimate interest</i>	<i>Why processing is necessary</i>	<i>Balance against interests, rights, freedoms</i>
Members	To maintain contact with our Members	To maintain contact with our Members	We provide a benefit to the Member. Membership is voluntary and can be withdrawn at any time.
Donors	To maintain contact with our Donors	To maintain contact with our Donors	Fundraising is a legitimate activity of SDM. Donors have opted to donate and can withdraw at any time.

Supporters	To maintain contact with our Supporters	To maintain contact with our Supporters	Fundraising is a legitimate activity of SWC. Supporters have opted to support us, and can withdraw at any time.
------------	---	---	---

## **Appendix 3 Privacy Notice for Employees, Workers and Contractors**

### **What is the purpose of this document?**

Stockport Women's Centre is committed to protecting the privacy and security of your personal information.

This privacy notice describes how we collect and use personal information about you during and after your working relationship with us, in accordance with the General Data Protection Regulation (GDPR).

It applies to all employees, workers and contractors.

Stockport Women's Centre is a "data controller". This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy notice.

This notice applies to current and former employees, workers and contractors. This notice does not form part of any contract of employment or other contract to provide services. We may update this notice at any time.

It is important that you read this notice, together with any other privacy notice we may provide on specific occasions when we are collecting or processing personal information about you, so that you are aware of how and why we are using such information.

## **Data protection principles**

We will comply with data protection law. This says that the personal information we hold about you must be:

1. Used lawfully, fairly and in a transparent way.
2. Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
3. Relevant to the purposes we have told you about and limited only to those purposes.
4. Accurate and kept up to date.
5. Kept only as long as necessary for the purposes we have told you about.
6. Kept securely.

## **The kind of information we hold about you**

Personal data, or personal information, means any information about an individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data).

There are "special categories" of more sensitive personal data which require a higher level of protection

We will collect, store, and use the following categories of personal information about you:

- Personal contact details such as name, title, addresses, telephone numbers, and personal email addresses.
- Date of birth.
- Gender.
- Next of kin and emergency contact information.
- National Insurance number.
- Bank account details, payroll records and tax status information.
- Salary, annual leave, pension and benefits information.
- Start date.
- Location of employment or workplace.
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process).
- Employment records (including job titles, work history, working hours, training records and professional memberships).
- Performance information.
- Disciplinary and grievance information.
- Information about your use of our information and communications systems in accordance with our IT policies.
- Photographs.

We may also collect, store and use the following "special categories" of more sensitive personal information:

- Information about your health, including any medical condition, health and sickness records.
- Information about criminal convictions and offences.

How is your personal information collected?

We collect personal information about employees, workers and contactors through the application and recruitment process, either directly from candidates or sometimes from an employment agency or background check provider. We may sometimes collect additional information from third parties including former employers, credit reference agencies or other background check agencies (such as DBS checks).

We will collect additional personal information in the course of job-related activities throughout the period of you working for us.

### **How we will use information about you**

*We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:*

- 1. Where we need to perform the contract we have entered into with you.*
- 2. Where we need to comply with a legal obligation.*
- 3. Where it is necessary for our legitimate interests (or those of a third party) and your interests and fundamental rights do not override those interests.*

*We may also use your personal information in the following situations, which are likely to be rare:*

- 1. Where we need to protect your interests (or someone else's interests).*

### **2. Where it is needed in the public interest or for official purposes.**

#### **Situations in which we will use your personal information**

We need all the categories of information in the list above primarily to allow us to perform our contract with you and to enable us to comply with legal obligations. In some cases we may use your personal information to pursue legitimate interests of our own or those of third parties, provided your interests and fundamental rights do not override those interests. The situations in which we will process your personal information are listed below:

- Making a decision about your recruitment or appointment.
- Determining the terms on which you work for us.
- Checking you are legally entitled to work in the UK.

- Paying you and, if you are an employee, deducting tax and National Insurance contributions.
- Providing any benefits to you.
- Liaising with your pension provider.
- Administering the contract we have entered into with you.
- Business management and planning, including accounting and auditing.
- Conducting performance reviews, managing performance and determining performance requirements.
- Making decisions about salary reviews and compensation.
- Assessing qualifications for a particular job or task, including decisions about promotions.
- Gathering evidence for possible grievance or disciplinary hearings.
- Making decisions about your continued employment or engagement.
- Making arrangements for the termination of our working relationship.
- Education, training and development requirements.
- Dealing with legal disputes involving you, or other employees, workers and contractors, including accidents at work.
- Ascertaining your fitness to work.
- Managing sickness absence.
- Complying with health and safety obligations.
- To prevent fraud.
- To monitor your use of our information and communication systems to ensure compliance with our IT policies.
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software distribution.
- Equal opportunities monitoring.

Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal information.

### **If you fail to provide personal information**

If you fail to provide certain information when requested, we may not be able to perform the contract we have entered into with you (such as paying you or providing a benefit), or we may be prevented from complying with our legal obligations (such as to ensure the health and safety of our workers).

### **Change of purpose**

We will only use your personal information for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If we need to use your personal information for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal information without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law

## **How we use particularly sensitive personal information**

*"Special categories" of particularly sensitive personal information require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal information. We may process special categories of personal information in the following circumstances:*

- 1. In limited circumstances, with your explicit written consent.*
- 2. Where we need to carry out our legal obligations and in line with our data protection policy.*
- 3. Where it is needed in the public interest, such as for equal opportunities monitoring or in relation to our occupational pension scheme, and in line with our data protection policy.*
- 4. Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards.*

*Less commonly, we may process this type of information where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public. We may also process such information about members or former members in the course of legitimate business activities with the appropriate safeguards.*

## **Our obligations as an employer**

We will use your particularly sensitive personal information in the following ways:

We will use information relating to leaves of absence, which may include sickness absence or family related leaves, to comply with employment and other laws.

We will use information about your physical or mental health, or disability status, to ensure your health and safety in the workplace and to assess your fitness to work, to provide appropriate workplace adjustments, to monitor and manage sickness absence and to administer benefits.

We will use information about your race or national or ethnic origin to ensure meaningful equal opportunity monitoring and reporting.

## **Do we need your consent?**

We do not need your consent if we use special categories of your personal information in accordance with our written policy to carry out our legal

obligations or exercise specific rights in the field of employment law. In limited circumstances, we may approach you for your written consent to allow us to process certain particularly sensitive data. If we do so, we will provide you with full details of the information that we would like and the reason we need it, so that you can carefully consider whether you wish to consent. You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us.

Information about criminal convictions

**We may only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.**

**Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.**

We will only collect information about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect information about criminal convictions as part of the recruitment process or we may be notified of such information directly by you in the course of you working for us.

We are allowed to use your personal information in this way to carry out our obligations if you might be working with vulnerable adults or children.

Data sharing

We may have to share your data with third parties, including third-party service providers.

We require third parties to respect the security of your data and to treat it in accordance with the law.

If we do, you can expect a similar degree of protection in respect of your personal information

**Why might you share my personal information with third parties?**

We will share your personal information with third parties where required by law, where it is necessary to administer the working relationship with you or where we have another legitimate interest in doing so.

"Third parties" includes third-party service providers (including contractors and designated agents). The following activities are carried out by third-party service providers:

## **How secure is my information with third-party service providers and other entities in our group?**

All our third-party service providers and other entities in the group are required to take appropriate security measures to protect your personal information in line with our policies. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

## **What about other third parties?**

We may also need to share your personal information with a regulator or to otherwise comply with the law.

## **Data security**

We have put in place measures to protect the security of your information. Details of these measures are available upon request from the Centre Manager of Stockport Women's Centre ("the Manager").

Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal information on our instructions and they are subject to a duty of confidentiality. Details of these measures may be obtained from the Manager.

We have put in place procedures to deal with any suspected data security breach and will notify you and any applicable regulator of a suspected breach where we are legally required to do so.

## **Data retention**

### **How long will you use my information for?**

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. Details of retention periods for different aspects of your personal information are available in our retention policy which is available from the Manager. To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you. Once you are no longer an employee, worker or contractor of the company we will retain and securely destroy your personal information in accordance with our data retention policy or applicable laws and regulations.

Rights of access, correction, erasure, and restriction

### **Your duty to inform us of changes**

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us.

### **Your rights in connection with personal information**

Under certain circumstances, by law you have the right to:

**Request access** to your personal information (commonly known as a "data subject access request"). This enables you to receive a copy of the personal information we hold about you and to check that we are lawfully processing it. The request can be made in writing or verbally. Full details of the subject access process can be obtained from the manager.

**Request correction** of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected.

**Request erasure** of your personal information. This enables you to ask us to delete or remove personal information where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal information where you have exercised your right to object to processing (see below). The request to erase your personal information can be made in writing or verbally.

**Object to processing** of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground. You also have the right to object where we are processing your personal information for direct marketing purposes.

**Request the restriction of processing** of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it.

**Request the transfer** of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we

transfer a copy of your personal information to another party, please contact the Manager preferably writing but this can be done verbally.

**What we may need from you**

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

**Right to withdraw consent**

In the limited circumstances where you may have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact the Manager, preferably in writing. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legitimate basis for doing so in law.

**Complaints**

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

**Changes to this privacy notice**

We reserve the right to update this privacy notice at any time, and we will provide you with a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information. **If you have any questions about this privacy notice, please contact the Manager.**

I, \_\_\_\_\_ (employee/worker/contractor name),  
acknowledge that on \_\_\_\_\_ (date), I received a  
copy of Stockport Women's Centre's Privacy Notice for employees, workers  
and contractors.

Signature .....

Name.....

## **Appendix 4 - Privacy Notice for Service Users**

**Your privacy is very important. This tells you about how we will collect, store and protect information we have about you.**

### **Where we will store information about you.**

Information about you, and details of the work we have done with you, will be stored on our Database record system, or on paper records. The information we hold could include:

- Some basic details, like your name, date of birth, address etc.
- Anything you tell us about yourself or your family
- Information other agencies such as the Police and Probation have told us about you if they have referred you to us.
- Details of your contact with us, and the support that you have been offered.
- Details of what you have achieved during your work with us

You have the right to see any information we have stored about you on our records, and you can ask to see a copy of those records by either a verbal or written request.

### **How will we protect your information?**

**Your information is protected, and our staff must work to strict rules about how they manage the information we have about you.**

The staff working with you, and their managers, would have access to your records. Also a small number of staff who have access to the whole record system for maintenance or data collection purposes. These people too must work within strict rules, so your information is always protected.

### **Sharing your information.**

**Normally, we would only share your information with other people or organisations when you have agreed that we can.**

However, there may be times when we would have a duty to share information about you, even if you do not agree. These would be:

- If we believe that either you, or someone else, was at risk of serious harm.
- If a legal body ordered us to share your information
- If you are working with us whilst being supervised by Probation Services, we would be obliged to share information with those services.

If we did have to share your information without you agreeing, you would be told what information had been shared, why, and with which agencies.

**At all other times we would need your written agreement before we could share your information.**

### **Equality Information.**

When you first come to with us, we will ask you to share information about yourself, such as your race and ethnicity, any disabilities you may have, your religion etc. We use this information to make sure that we offer an equal quality of service to everyone.

**You do not have to give us this information, but if you do, it will be stored on our record system.**

At any time, if you change your mind about us storing this information, you can ask us to remove it from our system.

### **Complaints and Queries**

If you have any questions or concerns about this Service User Privacy Notice or about how we process your personal data, please contact [admin@stockportwomenscentre.co.uk](mailto:admin@stockportwomenscentre.co.uk) or the Head of Service at Stockport Women's Centre.

You can also contact the ICO if you are unhappy with how we process your personal data. The ICO contact details are as follows:

Information Commissioner's Office  
Wycliffe House  
Water Lane  
Wilmslow  
Cheshire  
SK9 5AF

Helpline number: 0303 123 1113 ICO website: <https://www.ico.org.uk>

## **Appendix 5 - Subject Access Process**

### **What is a subject access request?**

An individual has the right to obtain a copy of their personal data as well as any supplementary information (most of which will be detailed in SWC's privacy statement). A subject access request helps people to understand how and why we are using their data and that we are doing so lawfully.

An individual is entitled to:

- Confirmation that we are processing their personal data
- A copy of the data held
- Supplementary information (which is included in SWC's Privacy Notice), including:
  - The purposes of processing individual data;
  - The categories of personal data we process;
  - The recipients/ categories of recipients that SWC discloses personal data to;
  - The retention period of personal data;
  - The existence of the right to request rectification, erasure or restriction or to object to such processing;
  - The right to lodge a complaint with the ICO;
  - Information on the source of data where the data obtained does not come directly from the individual;
  - The existence of any automated decision-making;
  - Safeguards that are in place relating to any personal data being transferred to a third country or international organisation.

### **How to recognise subject access requests**

An individual can make a request to SWC either verbally or in writing and can be made to anyone within the organisation (including via social media). The request does not have to contain the phrase 'subject access request' or make reference to GDPR as long as it is clear that the person is requesting their own personal data.

If someone receives such a request, SWC has chosen to use a Subject Access Request form. Anyone who makes such a request should be asked to complete the form and support should be offered to complete this if required.

## **Managing subject access requests**

All subject access requests should be recorded in the Subject Access file on the Shared Drive and a manager should be informed, who will then take on responsibility for overseeing the request. We cannot request a fee for completing subject access requests.

Legally we have one month to respond to a subject access request, although we can increase this by a further two months should there be multiple parts to a request or if the request is more complex. In cases where we will require longer than one month to complete the request, we must write to the requester within one month to explain why.

In terms of providing additional information with the request, GDPR states that the information we provide is concise, transparent, intelligible and easily accessible. Any additional information that we provide needs to be able to be understood by the 'average person'.

If SWC have processed a large amount of data concerning an individual, we are able to ask the individual to provide additional information about their request (for example, are they able to provide dates to which the request relates to?). We are not able to request that an individual narrows the scope of their request and they are entitled to request all the information we hold about them.

SWC may receive third party requests, such as requests from a solicitor, partner agency or family member. In such cases, SWC needs to be satisfied that the third party is entitled to act on behalf of the client; it is the third party's responsibility to prove this.

SWC may receive a subject access request where the data includes information about other people. The Data Protection Act 2018 states that we do not have to comply with the request if it means disclosing information that about another individual who can be identified, unless:

They have given consent

It is reasonable to comply without consent, in which case, SWC need to consider:

The type of information that would be disclosed;

Duty of confidentiality to the third party;

Steps taken to gain consent;

Is the third party able to give consent?

Has the third party refused consent?

### **Can SWC refuse a subject access request?**

SWC are able to refuse a request if:

It is manifestly unfounded;

It is excessive.

Requests should be assessed on a case by case basis and SWC must be able to demonstrate why this is the case and be able to explain this to the information commissioner.

A request can be considered to be manifestly unfounded if:

The individual has no intention to exercise their right of access (for example, they have stated they will withdraw it in exchange for something);

The request is malicious in intent and being used to harass/ cause disruption, for example;

The individual has stated, either in the request or elsewhere that they intend to cause disruption;

The request makes unsubstantiated accusations against SWC or its employees;

The individual is targeting particular employees;

The individual systemically sends different requests, for example on a weekly basis, as part of an ongoing campaign.

This is not a tick box exercise and each request should be considered on its own merit and SWC are responsible for demonstrating that it is manifestly unfounded. SWC should not assume that a request is manifestly unfounded just because the individual has previously made unfounded requests.

A request can be considered excessive if:

It repeats the substance of previous requests and a reasonable interval has not elapsed;

It overlaps with other requests.

However, it will not necessarily be excessive just because an individual:

Has requested a large amount of information; although this may be burdensome. We are able to ask the individual if they can clarify their request further;

Wants to receive a copy of the information previously provided; in such circumstances SWC are able to charge a fee for providing this information but we cannot consider this excessive;

Made an overlapping request relating to a separate piece of information;

Previously submitted requests that have been deemed excessive or manifestly unfounded.

In order to decide whether a reasonable time period has elapsed, SWC need to consider:

The nature of the data – including how sensitive this data is;

The purpose of processing the data, particularly if this information is likely to cause harm to the requester if disclosed;

How often data is altered – if the information is unlikely to have changed since the previous request, we may decide that we do not need to respond to the same request twice. If any data has been deleted in between requests, SWC needs to inform the individual.

In cases where SWC has made the decision to refuse the subject access request, the individual must be informed without undue delay and within one month of receipt of the request.

SWC should inform the individual of:

The reasons we are not taking action;

Their right to make a complaint to the ICO and any other supervisory body;

Their ability to seek and enforce this right through a judicial remedy.

## Appendix 1

### Requesting a copy of your records (Subject Access Request)

**Section 1 – Your details** (please note that it is an offence to impersonate someone.

**First Name**

**Surname**

**Previous Name(s)** (if applicable)

**Date of Birth**

**Telephone Number**

**Email Address**

**Address**

**Postcode**

If you have lived at this address for less than 2 years, please provide any previous addresses below:

### Section 2 – Your Request

To help us deal with your request as efficiently as possible, please write your request in as much detail as possible

### Section 3 – What we need from you

For all requests, we need documentary proof that you are who you say you are – this helps us protect your data by ensuring that we are dealing with you and that none of your personal information is accessed or interfered with by anyone else falsely claiming to be you. We will need 1 piece of photographic ID (driving licence, passport, etc) or 2 pieces of ID if you do not have this (Council tax letter, utility bill or bank statement).

#### **Section 4 – How to provide evidence**

You can send scanned copies of your ID/ consent via email to [admin@stockportwomenscentre.co.uk](mailto:admin@stockportwomenscentre.co.uk) or post copies to

Stockport Women’s Centre

39 Greek Street

Stockport

SK3 8AX

#### **Section 5 – Declaration of the Data Subject**

I can confirm that I am the data subject named and I am requesting information relating to my own personal data. I understand that the information I have supplied will be used to confirm my identity and help locate the information requested:

**Signed**

**Dated**

## Appendix 2

### Subject Access Request Record

Date of Initial Enquiry	Staff Member	Manager Responsible	Request Format (verbal/written)	Action Taken	Completion Date
