Cymorth i Ferched Cymru
Welsh Women's Aid
Rhoi Merched a Phlant yn Gyntaf
Putting Women & Children First

Standard Operating Procedure

Confidentiality, Data Protection and Sharing Information

Document Details **Welsh Women's Aid Internal**

Reference
WWA SOP- CDP&SI

Version
Final

Approval Date
01/06/2021

Date for next Review
01/05/2025

Accountability
All employees, Trustees, volunteers and consultants of Welsh Women's Aid

SOP Owner: Emma Harris, HR Manager
Author: Welsh Women's Aid's Data Protection Team

Contents

1.0 Purpose

Welsh Women's Aid (WWA) is committed to maintaining the highest standards of confidentiality in all of its work in order to ensure the safety and wellbeing of service users and staff.

WWA will:

- comply with both the law and good practice
- respect individuals' rights
- be open and honest with individuals whose data is held
- provide training and support for staff who handle personal data, so that they can act confidently and consistently
- Notify the Information Commissioner voluntarily, even if this is not required

We recognise that it is vital to work with other organisations to fulfil our obligations in respect of the safety and wellbeing of our service users. We will at all times endeavour to do this within the confines of legal requirements and best practice.

We also recognise the potential risks associated with breaches of confidentiality or inaccurate/insufficient information being provided, and that they may have life threatening consequences (among others).

WWA is committed to safeguarding the rights of service users and staff to access information, which is held about them and wherever possible gaining consent to share information about them within the legal and practice parameters set out in this document.

In fulfilling the above aims, WWA will work within the requirements of the following legislation:

1 The United Kingdom General Data Protection Regulation (UK-GDPR) 2020
2 The Data Protection Act 2018
3 The Human Rights Act 1998
4 The Children Act 1989
5 The Crime and Disorder Act 1998

Key elements and principles contained in the above pieces of legislation are set out in Appendix One for reference purposes.

Statutory and non-statutory retention periods are set out in Appendix Two and Three.

How to deal with a request for their data from a service user, staff member or member of the public is set out in Appendix 4.

2.0 Responsibilities	
The Board of Trustees	• Overall responsibility for ensuring that the organisation complies with its legal obligations.
Data Protection Officer	• Briefing the Board on Data Protection responsibilities • Reviewing Data Protection and related policies • Advising other staff on tricky Data Protection issues • Ensuring that Data Protection induction and training takes place • Notification to the ICO • Handling subject access requests • Approving unusual or controversial disclosures of personal data • Approving contracts with Data Processors
Senior Management Team	• Responsible for monitoring their own compliance with GDPR and reporting back to the DPO.
Employees & Volunteers	All staff and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work. (From now on, where 'staff' or 'employees' is used, this includes both paid workers and volunteers.)
Enforcement	• Staff will be provided with training and should ensure they remain up to date with any changes to policy or practice. • Any data breaches should be notified in line with this policy. • Data breaches will result in disciplinary action.

2.0 Procedures

2.1 Personal data

The GDPR applies to 'personal data' (as referenced in Article 10) which is defined by the Information Commissioners Office (ICO) as 'any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.'

The ICO goes on to state:
This definition provides for a wide range of personal identifiers to constitute personal data, including (but not limited to):

- name
- identification number
- location data
- online identifier

This reflects changes in technology and the way organisations like WWA collect information about people.

The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

Personal data that has been pseudonymised – e.g. key-coded – can also fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

2.2 Sensitive personal data

The GDPR refers to sensitive personal data as "special categories of personal data" (see Article 9).

The special categories specifically include genetic data, and biometric data where processed to uniquely identify an individual.

Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing (see Article 10)'.

3.0 The provisions of the GDPR

WWA is registered with the Information Commissioner's Office as a Data Controller, which means it 'determines the purposes and means of processing personal data' about its staff, volunteers, service users, supporters and other stakeholders. WWA is also a Data Processor, which means it is 'responsible for processing personal data'.

As a Data Controller, WWA is responsible for, and needs to be able to demonstrate, compliance, with the 5 principles of GDPR. These are listed under Article 5, and requires personal data held by WWA to be:
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."

(Taken from https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/)

The GDPR has significant impact on day-to-day activity in respect of gathering, using and sharing information. The key provisions are set out below.

3.1 Processing personal data – lawful basis

(adapted from https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/)

- WWA must have a valid lawful basis in order to process personal data (as detailed in Article 6). There are six available lawful bases for processing, and which basis we select will depend on the purpose and relationship with the individual.

- The lawful bases for processing are set out in Article 6 of the GDPR. At least one of these must apply whenever WWA process personal data:

  (a) Consent: the individual has given clear consent for WWA to process their personal data for a specific purpose.

  (b) Contract: the processing is necessary for a contract WWA has with the individual, or because they have asked WWA to take specific steps before entering into a contract.

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

  (d) Vital interests: the processing is necessary to protect someone's life.

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

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

3.2 'Necessary' processing

- Most lawful bases require that processing is 'necessary', which means that WWA must not reasonably be able to achieve the same purpose without processing the data. This does not mean that processing always has to be essential. However, it must be a targeted and proportionate way of achieving the purpose.

- It is not enough to argue that processing is necessary because you have chosen to operate your business in a particular way. The question is whether the processing is a necessary for the stated purpose, not whether it is a necessary part of your chosen method of pursuing that purpose.

When WWA will decide which lawful basis applies:

- WWA will determine the lawful basis **before** we begin processing the data, and will document it to ensure transparency and accountability in line with Articles 5(2) and 24.

- If processing special category data, criminal conviction data, or data about offences, WWA will identify both a **lawful basis** for general processing and an **additional condition** for processing this type of data.
- The data subject must be informed of the lawful process prior to collecting the data, or if the data is already held prior to the 25th May 2018.

3.3 Making a change to the legal basis for processing

- The 'purpose limitation' principle in Article 5, states that "personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes".

- However over time, if there is a genuine change in circumstances or a new purpose which WWA did not originally anticipate, WWA will review the lawful basis for collecting that data. WWA may not need to change the lawful basis if the new purpose is compatible with the original purpose. In this case, WWA will also consider whether it is fair and transparent, and give individuals information about the new purpose.

- If there is a change in the lawful basis, WWA will inform the individual and document the change.

- An exception to the above is if the legal basis is consent, as the GDPR specifically says that consent must always be specific and informed. So if the purpose changes, WWA will either get fresh consent which specifically covers the new purpose, or find a different basis for the new purpose.

In order to assess whether the new purpose is compatible with the original purpose WWA will take into account:

- any link between the initial purpose and the new purpose;
- the context in which we collected the data – in particular, our relationship with the individual and what they would reasonably expect;
- the nature of the personal data – eg is it special category data or criminal offence data;
- the possible consequences for individuals of the new processing; and
- whether there are appropriate safeguards - eg encryption or pseudonymisation.

This list is not exhaustive and what we will look at depends on the particular circumstances.

It should be noted that the GDPR specifically says that further processing for the following purposes should be considered to be compatible lawful processing operations:

- archiving purposes in the public interest;
- scientific research purposes; and
- statistical purposes.

How WWA will decide which lawful basis applies

WWA will consider which lawful basis best fits the circumstances, and if more than one basis applies. In such cases WWA will document all lawful basis.

WWA will consider a variety of factors, including:

- What is WWA's purpose for collecting the data and what are we trying to achieve?
- Could we reasonably achieve it in a different way?
- Do we have a choice over whether or not to process the data?

When moving towards legitimate interest or consent as a legal basis, we will also consider the following:

- Who does the processing benefit?
- Would individuals expect this processing to take place?
- What is WWA's relationship with the individual?
- Is WWA in a position of power over them?
- What is the impact of the processing on the individual?
- Are they vulnerable?
- Are some of the individuals concerned likely to object?
- Is WWA able to stop the processing at any time on request?

How WWA will document our lawful basis

The principle of accountability requires WWA to be able to demonstrate that we are complying with the GDPR, and which means that we need to be able to show that we have properly considered which lawful basis applies to each processing purpose and can justify the decision.

We will therefore keep a record of which basis we are relying on for each processing purpose, and a justification for why we believe it applies.

What we will tell data subjects

WWA will include information about our lawful basis (or bases, if more than one applies) in our privacy notice. Under the transparency provisions of the GDPR, the information we will give people includes:

- our intended purposes for processing the personal data; and
- the lawful basis for the processing.

This applies regardless of whether WWA collects the personal data directly from the individual or via another source.

3.4 Special category data and criminal offence data

When WWA processes special category data, we will identify both a lawful basis for processing and a special category condition for processing in compliance with Articles 9 and 10, both of which will be documented to ensure we can demonstrate compliance and accountability.

Special category data is personal data which the GDPR says is more sensitive, and so needs more protection.

In order to lawfully process special category data, WWA will identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9. These do not have to be linked.

Special category data includes:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

In particular, this type of data could create more significant risks to a person's fundamental rights and freedoms. For example, by putting them at risk of unlawful discrimination.

There are currently ten conditions for processing special category data in the GDPR under Article 9(2), and the relevant category/ies must be identified and recorded prior to collecting any data. https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/ (see appendix).

Those that are most relevant to data collected by WWA are as follows:

Explicit consent given: (a) the data subject has given **explicit consent** to the processing of those personal data for one or more specified purposes.

Necessary for employment or social security: (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of **employment and social security and social protection law**.

Legitimate activities: (d) processing is carried out in the course of its **legitimate activities** with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

Legal claim: (f) processing is necessary for the establishment, exercise or **defence of legal claims** or **whenever courts are acting in their judicial capacity;**

Substantial public interests: (g) processing is necessary for reasons of **substantial public interest**, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

Medical: (h) processing is necessary for the purposes of **preventive or occupational medicine**, for the **assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services** on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3.

4.0 Sharing information within an organisation and with outside bodies

https://ico.org.uk/for-organisations/data-sharing-a-code-of-practice/

By 'data sharing' we mean the disclosure of data from WWA to a third party organisation or organisations, or the sharing of data between different parts of WWA.

Data sharing is part of the wider function of data processing, as defined in Article 4.2

'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, , restriction, erasure or destruction; disclosure by transmission, dissemination or otherwise making available, alignment or combination

Data sharing and can take the form of:

- a reciprocal exchange of data;
- WWA providing data to a third party or parties;
- WWA joining several organisations in pooling information and making it available to each other;

- WWA joining several organisations pooling information and making it available to a third party or parties;
- exceptional, one-off disclosures of data in unexpected or emergency situations;
- different parts of WWA making data available to each other.

Some data sharing doesn't involve personal data, for example where only statistics that cannot identify anyone are being shared.

There are two main types of data sharing:

- systematic, routine data sharing where the same data sets are shared between the same organisations for an established purpose; and
- exceptional, one-off decisions to share data for any of a range of purposes.

Different approaches will need to apply to these two types of data sharing,

WWA may also decide, or be asked, to share data in situations which are not covered by any routine agreement. In some cases this may involve a decision about sharing being made in conditions of real urgency, for example in an emergency situation.

Sharing with a 'data processor'

When talking about data sharing we are normally referring to sharing personal data between controllers – i.e. where both organisations determine the purposes for which and the manner in which the personal data is processed.

However, a data controller can also share data with a data processor, who processes personal.

When a data controller such as WWA uses a data processor it must ensure, in a written contract, that:

- the processor only acts on instructions from the data controller; an
- that it has security in place that is equivalent to that imposed on the data controller by the seventh data protection principle.

Therefore, a data processor involved in data sharing doesn't have any direct data protection responsibilities of its own; they are all imposed on it through its contract with the data controller.

When considering sharing information, WWA will make use of the data sharing code of practice: https://ico.org.uk/for-organisations/data-sharing-a-code-of-practice/

Where a member of staff is unclear about any issues in this area they should consult their line manager.

When members of staff are required to share information with outside bodies they must ensure that they observe the steps set out below;

- the information must go directly to the right person – making sure that the information is marked private and confidential;

- make sure that they know who, if anyone, the information will be shared with by the recipient;
- they will ensure that the recipient understands the sensitivity and status of that information and knows what to do with it;
- they will ensure that the sharing of information is a private not public process;
- they will communicate with that person to ensure they understand the next steps and any further action;
- If the member of staff feels that as a consequence of sharing information another staff member or service user may be at risk, this must be discussed at a senior level within the organisation.

An information sharing protocol should be established with outside organisations with whom regular or repeated sharing is possible.

4.1 Sharing service user information when consent has been granted

Consent for information sharing is most likely to be needed where:

- confidential or particularly sensitive information is going to be shared without a clear legal basis for doing so;
- the individual would be likely to object should the data be shared without his or her consent; or
- the sharing is likely to have a significant impact on an individual or group of individuals.

WWA asks service users to give their consent (where consent is the legal basis for processing to share their information as part of the referral, application and assessment processes and this is renewed at review meetings.

In gaining consent:

- staff must be clear with the service user about why they want to share information about them and who it will be shared with;
- service users should have a chance to put their point of view and to ask any questions;
- such discussions should be recorded and service users should be asked to sign a consent form;
- where the service user refuses consent a record should also be kept. Where this is the case if staff have grounds to share the information without the service user's consent and intend to do so they should tell the service user of their intention unless there are good reasons not to do so such as jeopardising someone's safety;
- all such records should be kept on an individual's file;

Where information is to be shared which a member of staff knows may be contentious and/or it is of a 'sensitive' nature (see special category definition in section x) she must seek specific consent to share this information and to record this consent through obtaining the signature of the person alongside the date and issue on which consent is being sought.

If members of staff are unsure about what steps to follow and how to interpret the requirements set out below in any given situation they should consult their line manager who should seek external advice and guidance if necessary.

4.2 Communication with service users when you need to share their information without their consent

It is good practice to keep people informed of what is happening to their information, even if this is difficult. Experience shows that this increases trust and openness in relationships, and gives the service user a sense of control over what happens to them.

Where members of staff are sharing information without consent the individual should be told before the information is shared, unless this would:

- place someone at risk;
- prejudice a police investigation,
- lead to unjustifiable delay.

If one of these applies, let the person know as soon as it is possible, (if it is possible) and when it is safe to do so.

5.0 Interpreting the GDPR in respect of children

- Children need particular protection when collecting and processing their personal data because they may be less aware of the risks involved.
- When processing children's personal data, WWA will think about the need to protect them from the outset, and design our systems and processes with this in mind.
- Compliance with the data protection principles and in particular fairness is central to all our processing of children's personal data.
- WWA will decide upon the lawful basis for processing a child's personal data. Consent is one possible lawful basis for processing, but it is not the only option. Sometimes using an alternative basis is more appropriate and provides better protection for the child.
- If relying on consent as your lawful basis for processing personal data **when offering an online service directly to a child**, only children aged 13 or over are able provide their own consent. For children under this age WWA will gain consent from whoever holds parental responsibility for the child, **except where this relates to a preventive or counselling service**.
- With regard to gaining a child's consent in sharing information about them, the GDPR does not set down a precise age at which a child can act in her/his own right. However, as with online services, WWA has adopted the principle that consent should normally be gained from a parent/legal guardian unless the child is aged 13 or over and clearly understands what is involved and is capable of making an informed decision.
- In some situations where gaining consent from the parent may exacerbate a situation of actual or threatened harm to a child their consent will not be sought. It is therefore possible that in some circumstances action may be taken where consent has not been gained from the adult or the child. Where this takes place staff will ensure that the process and any actions are fully recorded.

- Children merit specific protection when you use their personal data for marketing purposes or creating personality or user profiles.
- WWA will write clear privacy notices for children so that they are able to understand what will happen to their personal data, and what rights they have.
- Children have the same rights as adults over their personal data. These include the rights to access their personal data; request rectification; object to processing and have their personal data erased.
- An individual's right to erasure is particularly relevant if they gave their consent to processing when they were a child.

It is clear from the above that a parent or legal guardian's consent can be overridden in respect of safeguarding the interests of her children – although as set out below, where possible, it would be helpful to gain her consent or/and keep her informed of actions. The Child Protection Procedures reinforce this approach.

In principle, where it is possible, a child's consent should be gained for sharing information about them. Where it is not possible to achieve informed consent they must be listened to, consulted and informed in general about what is happening. The communication must be sensitive and reflect a child's abilities to comprehend.

Where matters of Child Protection are concerned the actions of members of staff will be informed by this Policy and the requirements of the national Child Protection Procedures and any other requirements.

6.0 Rights of the individual

The GDPR provides the following rights for individuals:

1. The right to be informed

- Individuals have the right to be informed about the collection and use of their personal data.
- WWA will provide individuals with information including: our purposes for processing their personal data, our retention periods for that personal data, and who it will be shared with. This is called 'privacy information'.
- WWA will provide privacy information to individuals at the time we collect their personal data from them.
- If we obtain personal data from other sources, we will provide individuals with privacy information within a reasonable period of obtaining the data, and no later than one month.
- If an individual already has the privacy information, or if it would involve a disproportionate effort to provide it to them, we are allowed not to do so.
- The information WWA provides to people will be concise, transparent, intelligible, easily accessible, and it will use clear and plain language.
- We will regularly review, and where necessary, update our privacy information. We will bring any new uses of an individual's personal data to their attention before we start the processing.

2. The right of access

- All individuals have the right to access their personal data, or their children's personal data (unless to do so would place the child in a situation of potential or actual harm). This is called a Subject Access Request (SAR).
- WWA will ensure that a detailed record of all information processed is kept on a service user's or employee's file.
- Where this occurs and the child/young person is deemed competent, their permission should be sought. There is no single test for determining a young person's competence, however good practice guidelines recommend considering the following when assessing competence:
  - Applies to children aged 13 and over
  - Their ability to understand that there is a choice and that choices have consequences;
  - Their willingness and ability to make a choice (including the option that someone else make decisions for them);
  - Their understanding the nature and purpose of the proposed service;
  - Their understanding the alternatives to the service;
  - Their freedom from pressure.
- Individuals can make a subject access request (SAR) verbally or in writing.
- WWA will respond within one month to respond to a request.
- This information is normally provided free of charge.

3. The right to rectification

- Individuals have the right for inaccurate personal data to be rectified, or completed if it is incomplete.
- An individual can make a request for rectification verbally or in writing.
- WWA will respond to any request within one calendar month.
- In certain circumstances we can refuse a request for rectification.

4. The right to erasure (or the right to be forgotten)

- Individuals have the right to have their personal data erased.
- Individuals can make a request for erasure verbally or in writing.
- WWA will respond to any request within one month.
- The right is not absolute and only applies in certain circumstances.

5. The right to restrict processing

- Individuals have the right to request the restriction or suppression of their personal data.
- This is not an absolute right and only applies in certain circumstances.
- When processing is restricted, WWA is permitted to store the personal data, but not use it.
- An individual can make a request for restriction verbally or in writing.
- WWA will respond to any request within one calendar month.

6. **The right to data portability**
   - The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.
   - It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability.
   - Doing this enables individuals to take advantage of applications and services that can use this data to find them a better deal or help them understand their spending habits.
   - The right only applies to information an individual has provided to a controller.

7. **The right to object**
   - Individuals have the right to object to the processing of their personal data in certain circumstances.
   - Individuals have an absolute right to stop their data being used for direct marketing.
   - In other cases where the right to object applies, WWA may be able to continue processing if we can show that we have a compelling reason for doing so.
   - We will tell individuals about their right to object.
   - An individual can make an objection verbally or in writing.
   - WWA will respond to any objection within one calendar month.

8. **Rights in relation to automated decision making and profiling**
   There are provisions relating to:
   - Automated individual decision-making (making a decision solely by automated means without any human involvement); and
   - profiling (automated processing of personal data to evaluate certain things about an individual). Profiling can be part of an automated decision-making process.
   - WWA does not use any automated individual decision-making or profiling.

7.0 Other general issues in respect of confidentiality and the work of the organisation

The address of **refuges** will not be given out or discussed with anyone except in exceptional circumstances. The exceptions will be in the case of Social Services, the Housing Benefit authority, authorised contractors, health visitors etc, where legal requirements necessitate knowledge or direct access is required. WWA will attempt to minimize the number of people who know the refuge addresses by using the same contractors and dealing with the same person at an agency where possible.

Under no circumstances should the **work** of WWA be discussed in a non-professional situation outside of the working environment. This includes general conversation with work colleagues, friends and family.

Information on **service users** will be shared between staff, volunteers, Trustees and with outside bodies within the framework set out above. Where information is given to outside agencies or other individuals, members of staff will always ensure that they are certain that the individual is who they claim to be before disclosing any information. The same requirements apply in relation to **former service users**.

Under no circumstances will any personal information relating to **staff members, volunteers or Trustees** be given to any individual or organisation without the permission of that person.

8.0 Data recording and storage

Accuracy	It may worth setting out measures to ensure data accuracy. For example, where information is taken over the telephone, how is it checked back with the individual? If information is supplied by a third party, what steps will be taken to ensure or check its accuracy?
Updating	If there is a regular cycle of checking, updating or discarding old data, this should be mentioned. Please note the separate requirements for the data you hold. For example, you cannot keep CVs for more than 6 months unless you have express permission from the candidates
Storage	In **keeping information** on service users, staff, volunteers and Trustees, the information will be: • kept in locked cabinets; • protected by the use of passwords if stored electronically • recorded by codes if used for statistical purposes so those individuals remain anonymous.
Retention periods	See appendix
Archiving	The procedure for archiving or destroying data should be mentioned, along with any special considerations (see above)

All of the above will be informed about the systems, processes and protocols for keeping and using personal data that is being held about them when they first come into contact with the organisation.

To comply with the principles of the Data Protection Act, records containing personal data must be:

- stored appropriately having regard to the sensitivity and confidentiality of the material recorded

- collected for a specific purpose
- retrievable and easily traced
- retained for only as long as necessary

disposed of securely, this includes data held on paper and electronically, for example on CD's/Disks, or hard drives when they are replaced

9.0 Destruction and disposal procedures

All information should be destroyed when the specified time limits for the storage ends. This should be checked and reviewed on an annual basis to ensure compliance with the statutory and recommended time limits for storage. **Refer to Appendix for retention periods.**

All information, in any format, destroyed from any location must have due regard to confidentiality of our employees, volunteers and service users.

- When records or data files are identified for disposal in the Policy are destroyed, a register of such records needs to be kept.
- The procedure for the destruction of Confidential or Sensitive Waste on paper/card is as follows:
  - All confidential or sensitive paperwork should be mechanically shredded if the content is in any way sensitive.
  - If you dispose of waste by using the shredder, ensure that it is used safely in accordance with its operating instructions, and that waste is shredded in such a way that it cannot be put back together again, and made comprehensible, preferably using a cross shredder.
  - Alternatively an external confidential waste disposal company can be used, and the confirmation of destruction certificate should be kept on file.
  - Where information is kept electronically, ie. CD's/memory sticks, these should either be cleared or broken up.
  - When computers are disposed of, care must be taken to ensure no personal or sensitive data is left on the hard drive and secure disposal of the computer or hard drive should be arranged.

10.0 Passwords

WWA strives to obtain Cyber Essentials accreditation on an annual basis. In line with this passwords information should be kept by each individual and not disclosed to any other person inside or outside the organisation. Passwords should include letters, numbers, upper and lower cases and symbols for security.

On ending employment with WWA the user account will be disabled, relevant organisations will be informed to enable data protection protocols **immediately.**

11.0 Information and Training

All staff members, volunteers and Trustees will be trained in the use of this policy and procedure to ensure that confidentiality and access to information are dealt with appropriately at all times.

As part of registration with the Information Commissioner's Office, all staff will have signed the data protection training log to confirm they have received training in data protection to comply with the Information Commissioner's Office registration.

This will form part of all new employees, volunteers and Trustee's induction plan.

There will be an opportunities to raise Data Protection issues or concerns during employee training, team meetings, and supervisions.

12.0 Breaches of confidentiality

Any breaches of confidentiality will be proactively managed by the organisation, and staff, volunteers and Trustees will be given to understand that this may result in disciplinary action (where staff are concerned) and in a termination of their involvement with the organisation (volunteers and Trustees).

The paramount need to maintain confidentiality to maintain safety will be explained to service users when they first receive services from the organisation through a range of relevant paperwork such as the Refuge house rules, the Licence Agreement, the Refuge handbook and will be reinforced on a day to day basis. It will also be explained that any breaches may lead to action under the occupancy agreement and ultimately could result in their exclusion from the service.

WWA will also make the need to maintain the confidentiality of the refuge address, staff and service users clear to outside agencies and individuals. Where this is breached – Women's Aid will raise the issue with the organisation concerned and pursue the complaints process of that organisation where they are dissatisfied with the response. If no satisfactory outcome is achieved through the organisations complaint's process or there is a repeat violation, a complaint can be lodged with Information Commissioner.

A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

- Under the GDPR there is duty on all UK organisations to report certain types of personal data breach to the ICO.
- When a personal data breach has occurred, WWA will establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then we will notify the ICO within 72 hours.

- A breach should be reported using their helpline: **0303 123 1113**
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, WWA will also inform those individuals without undue delay.
- WWA will ensure we have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not we need to notify the relevant supervisory authority and the affected individuals.
- We will also keep a record of any personal data breaches, regardless of whether we are required to notify.
- If a WWA data processor suffers a breach, then they must inform you without undue delay as soon as they become aware. Details of the reporting process should be included in the contract that is in place.

13.0 Publicity and Public Relations

Staff must not reveal the location of properties to the media. Visits by external agencies must be kept to an absolute minimum.

Staff may not become involved with the media except with the express permission of the Director or Chair of Trustees.

14.0 Appendices

3.1 Legal basis for processing – in detail

- **Consent**

1. Consent means offering individuals real choice and control. Genuine consent should put individuals in charge, build trust and engagement, and enhance your reputation.
2. Consent requires a positive opt-in and WWA will not use pre-ticked boxes or any other method of default consent.
3. Explicit consent requires a very clear and specific statement of consent.
4. Consent requests will be kept separate from other terms and conditions.
5. WWA will be clear and concise when requesting consent.
6. WWA will name any third party controllers who will rely on the consent.
7. WWA will make it easy for people to withdraw consent and tell them how.
8. WWA will keep evidence of consent – who, when, how, and what we have told people.
9. The legal basis will be kept under review, and refreshed it if anything changes.
10. Where ever possible, WWA will avoid making consent to processing a precondition of a service.

- **Contract**

WWA will use consent as a lawful basis to process someone's personal data to fulfil our contractual obligations to them or because they have asked us to do something before entering into a contract (eg provide a quote).

- The processing must be necessary, and if we could reasonably do what they want without processing their personal data, this basis will not be applied.
- WWA will document our decision to rely on this lawful basis and ensure that we can justify your reasoning.
- If processing of special category data is necessary for the contract, WWA will identify a separate condition for processing this data.
- If the contract is with a child under 18, WWA will consider whether they have the necessary competence to enter into a contract. If there are doubts about their competence, WWA may consider an alternative basis such as legitimate interests, to help to demonstrate that the child's rights and interests are properly considered and protected.

- **Legal obligation**
- **Vital interests**
- **Public task**
- **Legitimate interest**

Human Rights Act 1998

The Human Rights Act 1998 (HRA) came into force in the United Kingdom on 1 October 2000. It incorporates the rights and freedoms set out in the European Convention on Human Rights. The English Courts must take into account decisions of the European Court of Human Rights.

Relevant Articles here are:
Article 6 - Right to a fair hearing – clients should be made aware of procedures, which enable them to see all relevant and appropriate information.

Article 8 – Right to respect for family and private life – unauthorised disclosure of a service user / client's record is a breach of this Article, although there are cases where exceptions are likely to apply.

Article 14 – Prohibition of discrimination – it would be in contravention of the HRA not to allow a person access to their records on the grounds of their sex, race, colour, membership of a political party etc. Also, information provided must be in a form accessible to those suffering from sensory impairments or those who cannot speak English or who may have other difficulties in understanding the information.

The Children Act 1989

Section 17, 47, and schedule 2 of the Children Act 1989 impose functions which Social Services Departments are legally obliged to undertake. In some circumstances other departments of the authority or other agencies are legally obliged to co-operate.

Sections 17 and 47 taken together impose a positive duty to safeguard and promote the welfare of children. Where there is a reasonable cause to suspect a child is suffering or is likely to suffer 'significant harm', Social Services are obliged to make all necessary enquires. Social Services are obliged to identify needs for services under Section 17. Information sharing is a crucial part of both processes.

The Crime and Disorder Act 1998

Section 115 of this act enables any person to disclose information to a relevant authority for the purpose of the prevention and reduction of crime and identification or apprehending of offenders.

3.2 Statutory Retention Periods

Record	Statutory retention period	Statutory authority
accident books, accident records/reports	3 years after the date of the last entry (see below for accidents involving chemicals or asbestos)	The Reporting of Injuries, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR) (SI 1995/3163)
accounting records	6 years for public limited companies	Section 221 of the Companies Act 1985
income tax and NI returns, income tax records and correspondence with the Inland Revenue	6 years after the end of the financial year to which they relate	The Income Tax (Employments) Regulations 1993 (SI 1993/744)
records relating to children	until the child reaches the age of 21 or until the child reaches 24 for child protection records	Limitation Act 1980
records relating to events notifiable under the Retirement Benefits Schemes (Information Powers) Regulations 1995, records concerning decisions to allow retirement due to incapacity, pension accounts and associated documents	6 years from the end of the scheme year in which the event took place, or the date upon which the accounts/reports were signed/completed.	The Retirement Benefits Schemes (Information Powers) Regulations 1995 (SI 1995/3103)
Statutory Maternity Pay records, calculations, certificates (Mat B1s) or other medical evidence	3 years after the end of the tax year in which the maternity period ends	The Statutory Maternity Pay (General) Regulations 1986 (SI 1986/1960)
Statutory Sick Pay records, calculations, certificates, self-certificates	3 years after the end of the tax year to which they relate	The Statutory Sick Pay (General) Regulations 1982 (SI 1982/894)
wage/salary records (also overtime, bonuses, expenses)	6 years	Taxes Management Act 1970

3.3 Recommended retention periods (i.e. where no statutory retention periods exist)

Record	Recommended retention period
Client records (if no children)	Up to 6 years from the date that the client leaves the service, in case of litigation for negligence
application forms and interview notes (for unsuccessful candidates)	at least 1 year
assessments under Health and Safety Regulations and records of consultations with safety representatives and committees	permanently
Inland Revenue approvals	permanently
money purchase details	6 years after transfer or value taken
parental leave	5 years from birth/adoption of the child or 18 years if the child receives a disability allowance
pension scheme investment policies	12 years from the ending of any benefit payable under the policy
personnel files and training records (including disciplinary records and working time records)	6 years after employment ceases
redundancy details, calculations of payments, refunds, notification to the Secretary of State	6 years from the date of redundancy.
senior executives' records (that is, those on a senior management team or their equivalents)	permanently for historical purposes
time cards	2 years after audit
trade union agreements	10 years after ceasing to be effective
trust deeds and rules	permanently
trustees' minute books	permanently
works council minutes	permanently

3.4 Sample Confidentiality Disclosure

We understand that confidentiality is important and we will always work to safeguard confidential information about you. This means that:

We will not share information about you or your children with anyone else unless we have your permission first. This is why we ask you to sign a disclosure form.

We will only ever break this rule if we are concerned for your safety and well-being and we need to get help or we believe you or your children are at risk of harm or if we are compelled to do so by a court of law or criminal investigation.

We will keep any information about you locked away and we will restrict access to that information to people with a need to know. This will include your Key Worker, your Child's Key Worker and any other people supporting you.

We will always work strictly to our Confidentiality Policy and the requirements of the Data Protection Act 1998. If you would like to see a full copy of our policy, please ask one of our Workers.

3.5 Subject Access Request

Section 7 of the Data Protection Act 1998 (the Act) gives individuals the statutory right, subject to some exemptions, to see information which organisations hold about them. SARs must be made in writing and accompanied by the statutory fee, if charged, currently set at a maximum of £10. There is a 40-day statutory maximum period allowed for responding to a SAR.

All SAR should be recorded appropriately, include time and date request taken and time it took to deal with the request. These records should be kept for a period of at least one year.

Verifying identity

You should always satisfy yourself as to the identity of a person making a SAR. Where the record is open and there is an ongoing relationship between professionals and the person making the SAR then you should consult with the key worker about the identity of the person.

SARs made by a representative

Anyone can authorise a representative to help them with a SAR. In some cases it will be enough to have a letter from the person nominating the individual as their representative.

However, many people who have accessed social services need representatives because they have physical, mental or emotional difficulties. Sometimes this can make them vulnerable. If you have reason to believe that someone is falsely claiming to act on behalf of a person making a SAR, you should investigate this before you disclose any information.

The 40-day response period

You must comply with an SAR promptly, in other words, as quickly as possible and in any event within 40 days of receipt of the request, or (if later), the receipt of:

- Confirmation of the identify of the person making the SAR or their authorised representative;
- the relevant fee (if charged maximum £10); or
- any necessary information to assist you in finding the information requested.

The 40 day response period is a statutory requirement and there are no exemptions.

Recording SAR handling
It is good practice to keep a record of exactly what information you have sent in response to a SAR, together with a note of information you have withheld and/or amended.. It is also good practice to make notes relating to how you reached these decisions and notes on any exemptions in the Act you relied on. These notes should also be kept with this record.

Keeping records on SAR handling will allow you to determine what information should be disclosed if a further SAR is received in the future and it will also help you in the event that you need to explain or justify the decisions made in respect of any SAR.

Exemptions
Exemptions to disclosure apply to any information that is processed for purposes concerned with:
i. Crime and taxation, where the disclosure might prejudice those purposes, ii. Negotiations, where the data comprise records of the intentions of an organisation that is negotiating with the Subject;

iii. Health, where in the opinion of a health professional disclosure might cause harm to the Subject;

iv. Adoption records relating to the Subject;

v. Legal professional privilege;

vi. Any matter where there is a substantial public interest in not disclosing the information.

Further information in relation to subject access requests and how to respond can be found on the ICO website: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

3.6 Data Protection: Model Letters Pack

Introduction
This pack contains model letters which may be used when processing subject access requests made under the Data Protection Act 1998. They are model letters and as such can be altered to suit particular circumstances. The model letters should be used in conjunction with WWA's request handling procedures:

- Dealing with a subject access request for references
- Receiving and responding to a subject access request (staff)
- Receiving and responding to a subject access request (practitioners)

The following model letters are included in this pack:

- Receiving and clarifying request
- Acknowledgement of request
- Obtaining a valid subject access request (fee and further information required)
- Obtaining a valid subject access request (fee only required)
- Obtaining a valid subject access request (further information only required)
- Verifying the identity of a data subject
- Looking for the information
- Internal letter requesting staff to search their records
- Obtaining and acknowledging the opinions of third parties
- Obtaining the opinions of a third party (including referees)
- Acknowledgment of the third party's consent to disclose the information
- Acknowledgment of the consideration of the third party's opinions regarding disclosure of the information and explanation of the decision reached
- Release and partial release
- Replying to a subject access request providing the requested information
- Release of part of the information when the remainder is covered by an exemption
- Replying to a subject access request explaining why you have only sent some of the requested references
- Refusal
- Replying to a subject access request explaining why you cannot provide any of the requested information
- Replying to a subject access request explaining that only references received by are liable for disclosure
- Replying to a subject access request explaining why you cannot provide the requested reference/s

Acknowledgment letter

[Name]

[Address]

[Date]

Dear [Name]

Thank you for your [letter/email/fax] of [date] requesting information about [subject]. I am writing to let you know that we have received your request and will process it as soon as possible, and certainly within 40 calendar days of the day we received the request. You will hear back from us by [calculate date by which WWA must have processed the request] at the latest.

Yours sincerely

Internal letter requesting staff to search their records

Dear

Data Protection Act: Subject access request

WWA has received a subject access request for the following information [details of requested information].

Please search your [paper records / e-mails / computer drives] and locate any relevant information.

WWA has a statutory deadline for responding to this request. Please return all relevant information to [name] by [date] along with a record of how long it has taken you to retrieve it.

Yours sincerely

Obtaining the opinions of a third party (including referees)

[Name]

[Address]

[Date]

Dear [Name of third party]

I am writing to seek your views on the disclosure to [name of data subject] of [give brief description of document/s].

We have received a subject access request from [name of data subject] under the Data Protection Act 1998. Under this Act [name of data subject] has a right to receive copies of the information we hold about [him/her] unless particular exemptions apply. These exemptions include information about third parties where the third parties' interest in the data remaining confidential is greater than [name of data subject] 's interest in receiving the data.

In our search we identified some records that involve you. Before disclosing substantive third party information it is our practice to seek the views of the third party concerned and to take these views into account when applying the exemption. [Name of data subject] has the right to challenge any non-disclosure decisions that we make. This means that we cannot guarantee that these records will not be disclosed. However, we will ensure that your views are taken into account in any discussion about their disclosure.

The items concerned are included in [describe file]. They are:

1. [Itemise the documents concerned or for large quantities list the number of pages]

I enclose copies of them for you information.

Please could you let me know whether or not you have any objections to the disclosure to [name of the data subject] of your [whatever the document is]? If you do have any objections, please could you explain their nature so that we can take your views into account when considering whether to disclose?

The Data Protection Act requires us to reply to [name of data subject] by [date – 40 days after receipt of valid subject access request], so I would be grateful if you could reply to my letter by [date – allow yourself enough time to weigh the issues and to reply].

If you would like clarification of any of the points I have raised, please feel free to contact me.

Yours sincerely

Acknowledgment of the third party's consent to disclose the information

[Name]

[Address]

[Date]

Dear [Name of referee]

[Name of data subject]

Thank you for your letter dated [date] concerning the disclosure of [whatever the document is] in response to [name of data subject's] data subject access request. As you have no objections to the release of the information, I will include it in the information that I supply to [name of data subject] in response to [his/her] subject access request.

Thank you for taking the time to consider this matter.

Yours sincerely

Acknowledgment of the consideration of the third party's opinions regarding disclosure of the information and explanation of decision reached

[Name]

[Address]

[Date]

Dear [Name of referee]

[Name of data subject]

Thank you for your letter dated [date] concerning the disclosure your [whatever the document is] in response to [name of data subject's] subject access request. Following consideration of your views we have decided [not to disclose the reference / to disclose an anonymised version of the reference / to disclose the reference].

[Explain how you came to your decision.]

Thank you for taking the time to consider this matter.

Yours sincerely

Obtaining a valid subject access request (fee and further information required)

[Name]

[Address]

[Date]

Dear [Name]

Thank you for your letter of [date] making a subject access request for [whatever information has been requested].

So that we can process your request we need some more information. [ask for further information which will assist you in locating the information]. Any further information you can supply will assist us in answering your request.

We intend to search in the following places but we need more information if this does not cover everything:

[list areas which will be searched]

We charge a £10 fee for responding to Data Protection requests. Cheques should be made payable to the "WWA". Please note that we cannot process your request until we have received the fee.

Yours sincerely

Obtaining a valid subject access request (fee only required)

[Name]

[Address]

[Date]

Dear [Name]

Thank you for your letter of [date] making a subject access request for [whatever information has been requested].

We charge a £10 fee for responding to Data Protection requests. Cheques should be made payable to the "WWA". Please note that we cannot process your request until we have received the fee.

Yours sincerely

Obtaining a valid subject access request (further information only required)

[Name]

[Address]

[Date]

Dear [Name]

Thank you for your letter of [date] making a subject access request for [whatever information has been requested].

So that we can process your request we need some more information. [ask for further information which will assist you in locating the information]. Any further information you can supply will also assist us in answering your request.

We intend to search in the following places but further information is needed if this does not cover everything:

[list areas which will be searched]

Yours sincerely

Verifying the identity of a data subject

A script for a telephone call to confirm the identity of an individual making a subject access request.

Good morning [name of data subject]

I am telephoning from the _ about the subject access request you have made under the Data Protection Act. My name is [your name] and I am processing your request.

Before we can accept your request, I have to confirm your identity. This is to make sure that we do not release your data to anyone other than yourself. Please could I ask you two questions, based on the information that we hold about you, to confirm your identity?

The first question is: [question 1]

The second question is: [question 2]

[If the person answers the questions correctly:]

Thank you for answering these questions correctly. I will note on our file that I have confirmed your identity, and I will start to process your request.

[If the person refused to answer the question:]

I am sorry, we cannot comply with your request until we have confirmed your identity. If you are not prepared to answer the questions, is there another way we could confirm your identity?

[If the person answers the question incorrectly:]

I am sorry, you answered question [1/2] incorrectly. Is there another way we could confirm your identity?

[Please record the telephone conversation on the form on the following page.]

Telephone call to confirm the identity of an individual making a subject access request

Please complete the form below.

Name of member of staff	
Name of data subject	
Telephone number	
Date of call	
Time of call	
Question 1: Reply:	

Question 2: Reply:
Outcome:

Replying to a subject access request providing the requested information

[Name]

[Address]

[Date]

Dear [Name of data subject]

Data Protection Act 1998 subject access request

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

We are pleased to enclose the information you requested.

Copyright in the information you have been given belongs to or to another party. Copyright material must not be copied, distributed, modified, reproduced, transmitted, published (including published on the Internet or an intranet), or otherwise made available in whole or in part without the prior written consent of the copyright holder.

Yours sincerely

Release of part of the information, when the remainder is covered by an exemption (excluding references – see letter 14)

[Name]

[Address]

[Date]

Dear [Name of data subject]

Data Protection Act 1998 subject access request

Thank you for your letter of [date] making a data subject access request for [subject]. I am pleased to enclose [some/most] of the information you requested. However you will notice that

[if there are gaps in the document]

parts of the document(s) have been blacked out.

[if there are fewer documents enclose]

I have not enclosed all of the information you requested.

This is because, although holds all of the information you requested, I cannot supply you with all of it as part of it is [explain why it is exempt].

Copyright in the information you have been given belongs to or to another party. Copyright material must not be copied, distributed, modified, reproduced, transmitted, published (including published on the Internet or an intranet), or otherwise made available in whole or in part without the prior written consent of the copyright holder.

Yours sincerely

[Name]

[Address]

[Date]

Dear [Name of data subject]

Data Protection Act 1998 subject access request

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

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

Since we have been unable to provide the information you requested I am returning the £10 fee you supplied with your request.

Yours sincerely

Replying to a subject access request explaining that only references received by the WWA are liable for disclosure

[Name]

[Address]

[Date]

Dear [Name of data subject]

Data Protection Act 1998 subject access request

Thank you for your letter of [date] making a data subject access request for references supplied by [insert organisation/person] in connection with your [job/voluntary worker] application.

I regret that I cannot provide the [reference/references] that you requested. This is because they are exempt from disclosure under the Data Protection Act. WWA is not required to disclose references written by WWA staff and sent to external organisations.

Since we have been unable to provide the information you requested I herewith return the £10 fee you supplied with your request.

Yours sincerely

Replying to a subject access request explaining why you have only sent some of the requested references

[Name]

[Address]

[Date]

Dear *[Name of data subject]*

Data Protection Act 1998 subject access request

Thank you for your letter of *[date]* making a data subject access request for the references we received in connection with your *[job]* application.

I am pleased to enclose *[whichever reference can be disclosed]*. However, I have not provided *[a copy/copies]* of *[one/some]* of the references you requested because *[one of your referees/ your referees]* withheld consent to disclose *[it/them]*.

Copyright in the information you have been given belongs to or to another party. Copyright material must not be copied, distributed, modified, reproduced, transmitted, published (including published on the Internet or an intranet), or otherwise made available in whole or in part without the prior written consent of the copyright holder.

Yours sincerely

Replying to a subject access request explaining why you cannot provide the requested reference

[Name]

[Address]

[Date]

Dear *[Name of data subject]*

Data Protection Act 1998 subject access request

Thank you for your letter of *[date]* making a data subject access request for the references we received in connection with your *[job/course]* application. I regret that I cannot provide the *[reference/references]* that you requested.

[If using on the third party data exemption-]

The Act requires us to take into account the interests of third parties before disclosing their information as part of a subject access request. In order to process your request we contacted your referees to obtain their views regarding the disclosure of their reference for you. Your referees withheld consent to disclose the references so I regret that I cannot provide them.

Since we have been unable to provide the information you requested I herewith return the £10 fee you supplied with your request.

Yours sincerely