GDPR (Data Protection) Policy

Privacy statement

West Cornwall Women's Aid (WCWA) needs to collect and use certain types of information about the Individuals or Service Beneficiaries who come into contact with WCWA in order to carry out our work. This personal information must be collected and dealt with appropriately whether it is collected on paper, stored in a computer database, or recorded on other material; WCWA is required by law to comply with the following legislation:

- General Data Protection Regulation 2018
- The Data Protection Act (1998)
- The Data Protection (Processing of Sensitive Personal Data) Order 2000.

WCWA processes personal information for certain legitimate business purposes which includes some or all of the following:

- where the processing enables us to enhance, modify, personalise or otherwise improve our services for the benefit of our Service Beneficiaries, staff and volunteers
- to identify and prevent fraud
- to enhance the security of our network and information systems
- to better understand how people interact with our social media outlets
- to provide postal communications which we think will be of interest to you
- to determine the effectiveness of our promotional campaigns and advertising

Whenever we process data for these purposes we will ensure that we always keep your Personal Data rights in high regard and take account of these rights. You have the right to object to this processing if you wish to, and if you wish to do so please contact the line manager of the service you are involved with. Please bear in mind that if you object this may affect our ability to carry out tasks above for your benefit.

Data Controller

Cornwall Council (Safer Cornwall) is the Data Controller for refuge provision under the Act, which means that it determines what purposes personal information held, will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for.

WCWA is the Data Controller for Life Chances Project under the Act, which means that it determines what purposes personal information held, will be used for. It is also responsible for notifying the Information Commissioner of the data it holds or is likely to hold, and the general purposes that this data will be used for. Life Chances staff and volunteers input records onto a secure cloud based case management system; each member has their unique password for access. The case management system has been assessed against the HMG Baseline Controls which correspond to the good commercial practices described by ISO27001/2.

Disclosure

WCWA shares data with other agencies such as the local authority, funding bodies and other voluntary agencies.

The Service Beneficiary will be made aware in most circumstances how and with whom their information will be shared. There are circumstances where the law allows WCWA to disclose data (including sensitive data) without the data subject's consent.

These are:

a) Carrying out legal duty or as authorised by the Secretary of State
b) Protecting vital interests of an Individual/Service Beneficiary or other person
c) The Individual/Service Beneficiary has already made the information public
d) Conducting any legal proceedings, obtaining legal advice or defending any legal rights
e) Monitoring for equality and diversity purposes – eg. race, disability or religion
f) Providing a confidential service where the Individual/Service Beneficiary's consent cannot be obtained or where it is reasonable to proceed without consent: e.g. where we would wish to avoid forcing stressed or ill Individuals/Service Beneficiaries to provide consent signatures.

Emergency or life-threatening situations may warrant the sharing of relevant information with the relevant emergency services without consent. WCWA can use their own judgement to process personal data for safeguarding purposes, without consent if it's justified, to protect a child or an adult at risk, under the legal basis of vital interest.

WCWA regards the lawful and correct treatment of personal information as very important to successful working and to maintaining the confidence of those with whom we deal.

WCWA intends to ensure that personal information is treated lawfully and correctly.

To this end, WCWA will adhere to the Principles of Data Protection, as detailed in the Data Protection Act 2018.
Specifically, the Principles require that personal information:
Shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met
Shall be obtained only for one or more of the purposes specified in the Act, and shall not be processed in any manner incompatible with that purpose or those purposes

a) Shall be adequate, relevant and not excessive in relation to those purpose(s)
b) Shall be accurate and, where necessary, kept up to date
c) Shall not be kept for longer than is necessary
d) Shall be processed in accordance with the rights of data subjects under the Act
e) Shall be kept secure by the Data Controller who takes appropriate technical and other measures to prevent unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal information
f) Shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of Individuals/Service Beneficiaries in relation to the processing of personal information

WCWA will, through appropriate management and strict application of criteria and controls:

a) Observe fully conditions regarding the fair collection and use of information
b) Meet its legal obligations to specify the purposes for which information is used
c) Collect and process appropriate information, and only to the extent that it is needed to fulfill its operational needs or to comply with any legal requirements
d) Ensure the quality of information used
e) Ensure that the rights of people about whom information is held can be fully exercised under the Act
f) Take appropriate technical and organisational security measures to safeguard personal information

g) Ensure that personal information is not transferred abroad without suitable safeguards
h) Treat people justly and fairly whatever their age, religion, disability, gender, sexual orientation or ethnicity when dealing with requests for information
i) Set out clear procedures for responding to requests for information

These include:

- The right to be informed that processing is being undertaken
- The right of access to one's personal information
- The right to prevent processing in certain circumstances
- The right to correct, rectify, block or erase information which is regarded as wrong information

Data collection

Informed consent is when:-

- A Service Beneficiary clearly understands why their information is needed, who it will be shared with, the possible consequences of them agreeing or refusing the proposed use of the data
- Service Beneficiary then gives their consent

WCWA will ensure that data is collected within the boundaries defined in this policy. This applies to data that is collected in person, or by completing a form

When collecting data WCWA will ensure that the Individual/Service Beneficiary:

a) Clearly understands why the information is needed
b) Understands what it will be used for and what the consequences are should the Individual/Service Beneficiary decide not to give consent to processing

c) As far as reasonably possible, grants explicit consent, either written or verbal for data to be processed
d) Is, as far as reasonably practicable, competent enough to give consent and has given so freely without any duress
e) Has received sufficient information on why their data is needed and how it will be used

Data Storage

Information and records relating to Service Beneficiaries will be stored securely and will only be accessible to authorized personnel. Information relating to Service Beneficiaries shall not be stored on storage devices such as memory sticks.

Information will be stored only for as long as it is needed or required statute and will be disposed of appropriately.

It is WCWA responsibility to ensure all personal and company data is non-recoverable from any computer system previously used within the organisation which has been passed on/sold to a third party.

Physical Security
WCWA will ensure that:-

- Appropriate locks or other physical controls to the doors and windows of rooms where computers are kept
- Laptops are not left unattended at any time. Laptops must be stored securely in a lockable container when not in use
- Service Beneficiaries are never left alone with a laptop
- Only WCWA supplied media storage devices should be used on any computers
- All business critical information from media such as CD's will be removed before disposal
- All business critical information is removed from the hard drives of any computer before disposal
- Back up of business-critical information is stored either in a secure place off site or in a fire and water proof container

Access Controls

WCWA will ensure that staff:-

- Use unique passwords that are not obvious and change them regularly
- Use passwords that contain letters in both upper and lower case, numbers and special keys, and are six or more characters in length
- Never write down passwords or share this detail with anyone.

Awareness, Training and Security Checks in relation to personnel

WCWA will:-

- Perform integrity checks on all new employees to ensure that the information they have provided about their background, experience or qualifications is accurate
- Give all new employees an introduction to information security, and ensure that they read and understand this information security policy – this training will be provided by an external specialist contractor
- Ensure employees know where to find details of the information security standards and procedures relevant to their role and responsibilities
- Ensure that employees have access only to the information assets they need to do their jobs. When dismissing employees ensure that they do not take with them any business critical information
- Ensure that employees know about the common methods that can be used to compromise our system

Security and privacy technologies

WCWA will ensure that:

- All computers have anti-virus software installed and the virus definitions are updated once a week. All incoming and outgoing traffic must be scanned for viruses, as should any disk or CD that is used.
- Computers are regularly scanned for viruses
- A software firewall is in use
- All laptops are password protected and encrypted
- Users do not have sight/access to other user's logins (unless authorized for a specific purpose)
  The data bases used have an access authorisation statement displayed, each time a user logs-in, requiring user's agreement to comply with Data Protection and Information Governance

Incident/Response Management

WCWA will ensure that:

- Employees understand what is meant by a security breach incident, are able to recognise the signs and understand the need to notify management

- All breaches of this policy and any other information security incidents shall be reported to CEO
- If required as a result of an incident, data will be isolated to facilitate forensic examination. This decision shall be made by CEO
- Information security incidents shall be recorded by CEO to establish their cause and impact with a view to avoiding similar events. This policy shall be updated if required to reduce the risk of a similar incident re-occurring

Data access and accuracy

Service Beneficiaries have the right to access the information WCWA holds about them. WCWA will also take reasonable steps ensure that this information is kept up to date by asking data subjects whether there have been any changes.
In addition, WCWA will ensure that:

- It has a Data Protection Officer with specific responsibility for ensuring compliance with Data Protection. The Data Protection Officer if George Harris and can be contacted at info@dataprivacyservices.co.uk
- Everyone processing personal information understands that they are contractually responsible for following good data protection practice
- Everyone processing personal information is appropriately trained to do so
- Everyone processing personal information is appropriately supervised
- Anybody wanting to make enquiries about handling personal information knows what to do
- It deals promptly and courteously with any enquiries about handling personal information
- It describes clearly how it handles personal information
- It will regularly review and audit the ways it hold, manages and uses personal information
- It regularly assesses and evaluates its methods and performance in relation to handling personal information
- All staff are aware that a breach of the rules and procedures identified in this policy may lead to disciplinary action being taken against them

This policy will be updated as necessary to reflect best practice in data management, security and control and to ensure compliance with any changes or amendments made to the Data Protection Act 1998/GDPR 2018.

December 2020 onwards – Working From Home

All staff and volunteers have given assurances that if/when they have to work from home, they have access to a private and confidential space to safely carry out their work. Staff and volunteers have contract mobile phone provided by WCWA. An expenses plan is in place to reimburse any volunteers incurring additional costs (utilities) carrying out work on behalf of WCWA.
All staff working from home will do so on equipment supplied by WCWA. Staff are not permitted to use their personal equipment for such purposes. All laptops supplied by WCWA will be password protected and encrypted.
Life Chances staff and volunteers input records onto a secure cloud based case management system; each member has their unique password for access.
Refuge case management system is owned and managed by Safer Cornwall; each member of staff has their own unique password and secret word for accessing the system.

Social Media
WCWA's social media accounts may only be used by authorised staff for business purposes. Authorised users of business social media accounts shall be appropriately trained and be aware of the risks of sharing sensitive information via social media.

WCWA staff must behave responsibly while using any social media whether for business or personal use, bearing in mind that they directly or indirectly represent the company. If in doubt, consult line manager.

In case of any queries or questions in relation to this policy please contact:

Refuge Manager
PO Box 94
Penzance
TR18 2XP
refugemanager@wcwaid.co.uk

WCWA CEO
PO Box 94
Penzance
TR18 2XP
manager@wcwaid.co.uk

Document Control	
Issued/reviewed	Reviewed 25th August 2023
Author(s)	Rhiannon Jones Hayley Harris, Data Privacy Services
Approved	31st August 2023, Board of Trustees
Next review date (must be less than 3 years from previous version date)	1st July 2024