Wiltshire Community Care User Involvement Network (WSUN)

Controlled Document

Document Name:	**Data Protection Policy**
Document Reference Number:	**POL1**
Document Version Number (Which replaces previous Data Protection and IT Policy)/	1
Approved by Board of Trustees on:	May 2018
Review Schedule	Every year
Next review due	May 2020
Owner (Responsibility)	Louise Rendle, Chief Executive
Revision History	See appendix
Document Location	

Document Description

This document outlines our legal requirements under the General Data Protection Regulations and the processes for how WSUN meets them. Note: until GDPR come into force on 28 May 2018 the current Data Protection Act 2000 will continue to apply.

Implementation and Quality Assurance

Implementation is immediate and this Policy shall stay in force until any alterations are formally agreed.

The Policy will be reviewed every year by the Management Committee, sooner if legislation, best practice or other circumstances indicate this is necessary.

All aspects of this Policy shall be open to review at any time. If you have any comments or suggestions on the content of this policy please contact Louise Rendle at WSUN, The Independent Living Centre, Semington, BA14 6JQ 01380 871800

Data Protection Policy

Introduction

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the European Council and the European Commission intend to strengthen and unify data protection for individuals within the European Union (EU). It also addresses the export of personal data outside the EU. The primary objectives of the GDPR are to give citizens back control of their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU. When the GDPR takes effect it will replace the data protection directive (officially Directive 95/46/EC) from 1995. The regulation was adopted on 27 April 2016 and applies from 25 May 2018 after a two-year transition period..

The 1998 Data Protection Act, which came into force on 1 March 2000, will continue to apply until the new General Data Protection Regulations come into force in May 2018.

The following guidance is not a definitive statement on the Regulations, but seeks to interpret relevant points where they affect WSUN.

The Regulations cover both written and computerised information and the individual's right to see such records.

It is important to note that the Regulations also cover records relating to staff and volunteers.

All WSUN staff are required to follow this Data Protection Policy at all times.

The Chief Executive has overall responsibility for data protection within WSUN but each individual processing data is acting on the controller's behalf and therefore has a legal obligation to adhere to the Regulations.

Definitions

Processing of information – how information is held and managed.
Information Commissioner - formerly known as the Data Protection Commissioner.
Notification – formerly known as Registration.
Data Subject – used to denote an individual about whom data is held.
Data Controller – used to denote the entity with overall responsibility for data collection and management. WSUN is the Data Controller for the purposes of the Act.
Data Processor – an individual handling or processing data
Personal data – any information which enables a person to be identified

Special categories of personal data – information under the Regulations which requires the individual's explicit consent for it to be held by the Charity.

Data Protection Principles

As data controller, WSUN is required to comply with the principles of good information handling.

These principles require the Data Controller to:

1. Process personal data **fairly**, **lawfully and in a transparent manner.**
2. Obtain personal data only for one or more **specified** and **lawful purposes** and to ensure that such data is not processed in a manner that is incompatible with the purpose or purposes for which it was obtained.
3. Ensure that personal data is **adequate**, **relevant and not excessive** for the purpose or purposes for which it is held.
4. Ensure that personal data is **accurate** and, where necessary, **kept up-to-date.**
5. Ensure that personal data is not kept for any longer than is necessary for the purpose for which it was obtained.
6. Ensure that personal data is kept secure.
7. Ensure that personal data is not transferred to a country outside the European Economic Area unless the country to which it is sent ensures an adequate level of protection for the rights (in relation to the information) of the individuals to whom the personal data relates.

Consent

WSUN must record service users' explicit consent to storing certain information (known as 'personal data' or 'special categories of personal data') on file. *(See Article 9 GDPR Processing of special categories of personal data for more information*)

Special categories of personal information collected by WSUN will, in the main, relate to service users' physical and mental health. Data is also collected on ethnicity and held confidentially for statistical purposes.

Consent is not required to store information that is not classed as special category of personal data as long as only accurate data that is necessary for a service to be provided is recorded.

As a general rule WSUN will always seek consent where personal (Name, address and contact details) or special categories of personal information is to be held.

It should also be noted that where it is not reasonable to obtain consent at the time data is first recorded and the record remains open, retrospective consent will be sought at the earliest appropriate opportunity.

If personal and/or special categories of personal data need to be recorded for the purpose of service provision and the service user refuses consent, the case should be referred to the Chief Executive for advice.

Obtaining Consent

Consent may be obtained in a number of ways depending on the nature of the interview, and consent must be recorded on or maintained with the case records:

- face-to-face
- written
- telephone
- email.

Face-to-face/written

A pro-forma will be used.

Telephone

Verbal consent will be sought and noted on the case record. (But this must only be used in exceptional circumstances)

E-mail

The initial response will seek consent.

Consent obtained for one purpose cannot automatically be applied to all uses e.g. where consent has been obtained from a service user in relation to information needed for the provision of that service (e.g. WITS/BANES, Travel Support), separate consent would be required if, for example, WSUN wanted to include them in engagement activities.

Preliminary verbal consent will be sought at point of initial contact as personal and/or special categories of personal data will need to be recorded either in an email or on a computerised record (e.g. Lamplight). The verbal consent is to be recorded in the appropriate fields on the computer record or stated in the email for future reference. Although written consent is the optimum, verbal consent is the minimum requirement.

Specific consent for use of any photographs and/or videos taken will be obtained in writing. Such media could be used for, but not limited to, publicity material, press releases, social media, and website. Consent will also indicate whether agreement has been given to their name being published in any associated publicity. If the subject is less than 18 years of age then parental/guardian consent will be sought.

Individuals have a right to withdraw consent at any time. If this affects the provision of a service(s) by WSUN then the Staff member will discuss with the Chief Executive at the earliest opportunity.

Ensuring the Security of Personal Information

Unlawful disclosure of personal information

1. It is an offence to disclose personal information 'knowingly and recklessly' to third parties.

2. It is a condition of receiving a service that all service users for whom we hold personal details sign a consent form allowing us to hold such information.

3. Service users may also consent for us to share personal or special categories of personal information with other helping agencies on a need to know basis.

4. A client's individual consent to share information will always be checked before disclosing personal information to another agency.

5. Where such consent does not exist information may only be disclosed if it is in connection with criminal proceedings or in order to prevent substantial risk to the individual concerned. In either case permission of the Chief Executive will first be sought.

6. Personal information will only be communicated within WSUN's staff and volunteer team on a strict need to know basis. Care should be taken that conversations containing personal or special categories of personal information may not be overheard by people who should not have access to such information.

Ethnic Monitoring

In order for WSUN to monitor how well our staff, volunteers and service users reflect the diversity of the local community we request that they complete an options form for members or equal opportunity monitoring form. The completion of the form is voluntary, although strongly encouraged. Responses are securely stored and held on a pass-worded database for statistical purposes.

Use of Files, Books and Paper Records

In order to prevent unauthorised access or accidental loss or damage to personal information, it is important that care is taken to protect personal data. Paper records will be kept in locked cabinets/drawers overnight and care should be taken that personal and special categories of personal information is not left unattended and in clear view during the working the day. If your work involves you having personal / and/orspecial categories of personal data at home or in your car, the same care needs to be taken.

Disposal of Scrap Paper, Printing or Photocopying Overruns

Be aware that names/addresses/phone numbers and other information written on scrap paper are also considered to be confidential. Please do not keep or use any scrap paper that contains personal information but ensure that it is shredded.

If you are transferring papers from your home, or your client's home, to the office for shredding this needs to be done as soon as possible and not left in a car for a period of time. When transporting documents they should be carried out of sight in the boot of your car.

Computers

Where the information is stored on our Cloud-based Customer Relationship Management System (Lamplight), access to personal and special categories of personal information is restricted by levels of permissions and by password to authorised personnel only.

Where laptops are used in public areas, laptop screens will be positioned in such a way so that passers-by cannot see what is being displayed. If this is not possible then privacy screens will be used on the monitor to afford this level of protection. If working in a public area, you will lock your computer when leaving it unattended.

Firewalls and virus protection to be employed at all times to reduce the possibility of hackers accessing our system and thereby obtaining access to confidential records.

Where computers or other mobile devices are taken for use off the premises the device must be password protected.

Cloud Computing

When commissioning cloud based systems, WSUN will satisfy themselves as to the compliance of data protection principles and robustness of the cloud based providers.

The following privacy statement is to be included on any forms used to obtain personal data: **We promise never to share or sell your information to other organisations or businesses and you can opt out of our communications at any time by telephoning 01380 871800, writing to Louise Rendle at WSUN, The Independent Living Centre, Semington, BA14 6JQ or by sending an email to info.wsun@btconnect.com**

Privacy Statements

Any documentation which gathers personal and/or special categories of personal data will contain the following Privacy Statement information:

- Explain who we are
- What we will do with their data
- Who we will share it with
- How long we will keep it for
- That their data will be treated securely
- How to opt out
- Where they can find a copy of the full notice

A fuller Privacy Statement will also be published on our website. *Needs writing

Personnel Records

The Regulations apply equally to volunteer and staff records. WSUN may at times record special categories of personal data with the volunteer's consent or as part of a staff member's contract of employment.

For staff and volunteers who are regularly involved with vulnerable adults, it will be necessary for WSUN to apply to the Disclosure & Barring Service to request a disclosure of spent and unspent convictions, as well as cautions, reprimands and final warnings held on the police national computer. Any information obtained will be dealt with under the strict terms of the DBS Code. Access to the disclosure reports is limited to the Chief Executive and Finance Manager. If there is a positive disclosure the Chief Executive will discuss this, anonymously, with the Management Committee Chair and Vice Chair/s and our insurers to assess the risk of appointment. Management Committee members will not see the report itself.

Confidentiality

Further guidance regarding confidentiality issues can be found in our Confidentiality Policy.

When working from home, or from some other off-site location, all data protection and confidentiality principles still apply. All computer data, e.g. documents and programmes related to work for WSUN will not be stored on any external hard disk or on a personal

computer. If documents need to be worked on a personal computer, they will be saved onto a USB drive which will be password protected. (this will be only in exceptional circumstances)

Workstations in areas accessible to the public, e.g. Community Hubs, will operate a clear desk practice so that any paperwork, including paper diaries, containing personal and/or special categories of personal data is not left out on the desk where passers-by could see it.

When sending emails to outside organisations, e.g. social worker or GP surgery, care will be taken to ensure that any identifying data is removed and that codes (e.g. initials) are to be used. Confidential and/or special categories of personal information will be written in a separate document which will be password protected before sending. Wherever possible, this document will be 'watermarked' confidential.

Any paperwork kept away from the office (eg clients details kept at home by a worker) should be treated as confidential and kept securely as if it were held in the office. Documents should not be kept in open view (eg on a desktop) but kept in a locked metal box, the optimum being a locked cabinet but safely out of sight is a minimum requirement.

If you are carrying documents relating to a number of members/clients, you will keep the documents for other members/clients locked out of sight in the boot of the car (not on the front seat) and not take them into other members/clients home. When carrying paper files or documents they will be in a locked briefcase or in a folder or bag which can be securely closed or zipped up and padlocked. The briefcase/folder/bag will contain WSUN's contact details. Never take more personal data with you than is necessary for the job in hand. Care should be taken to ensure that you leave a member's/client's home with the correct number of documents and that you haven't inadvertently left something behind.

Retention of Records

Paper records will be retained for the following periods at the end of which they will be shredded:

- Member's/Client's records - 6 years after ceasing to be a member/client.
- Staff records – 6 years after ceasing to be a member of staff.
- Unsuccessful staff application forms – 6 months after vacancy closing date.
- Volunteer records – 6 years after ceasing to be a volunteer.
- Timesheets and other financial documents – 7 years.
- Employer's liability insurance – 40 years.

- Other documentation, eg clients benefit details or educational assessments sent to a worker as briefing for a visit, will be destroyed as soon as it is no longer needed for the task in hand.

Archived records will clearly display the destruction date.

Computerised records to be anonymised 6 years after ceasing to have any services from us. (Anonymising will remove the personal and special categories of personal data but will not remove the statistical data.)

What to Do If There Is a Breach

If you discover, or suspect, a data protection breach you will report this to your line manager who will review our systems, in conjunction with the Chief Executive, to prevent a reoccurrence. The Chief Executive will be informed of the breach, action taken and outcomes to determine whether it needs to be reported to the Information Commissioner and also for reporting to the Management Committee. There is a 72hr time limit for reporting breaches to the ICO so the Chief Executive and Management Committee will be informed without delay. More details can be found at https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/security-breaches/

Any deliberate or reckless breach of this Data Protection Policy by an employee or volunteer may result in disciplinary action which may result in dismissal.

If you have experienced a cyber crime you need to report this to Action Fraud https://www.actionfraud.police.uk any time of the day or night using their online reporting tool. Reporting is quick and easy. The tool will guide you through simple questions to identify what has happened and the advisors are available on web chat 24hours a day to give help and advice.

For more information about Cyber Attacks visit http://www.nationalcrimeagency.gov.uk/crime-threats/cyber-crime/online-safety-guidance-for-businesses

The Rights of an Individual

Under the Regulations an individual has the following rights with regard to those who are processing his/her data:

- Personal and special categories of personal data cannot be held without the individual's consent (however, the consequences of not holding it can be explained and a service withheld).

- Individuals have a right to have their data erased and to prevent processing in specific circumstances:
    - Where data is no longer necessary in relation to the purpose for which it was originally collected
    - When an individual withdraws consent
    - When an individual objects to the processing and there is no overriding legitimate interest for continuing the processing
    - Personal data was unlawfully processed
    - An individual has a right to restrict processing – where processing is restricted, WSUN is permitted to store the personal data but not further process it. WSUN can retain just enough information about the individual to ensure that the restriction is respected in the future.
- An individual has a 'right to be forgotten'.

Data Subjects can ask, in writing to the Chief Executive, to see all personal data held on them, including e-mails and computer or paper files. The Data Processor (WSUN) must comply with such requests within 30 days of receipt of the written request.

Powers of the Information Commissioner

The following are criminal offences, which could give rise to a fine and/or prison sentence

- The unlawful obtaining of personal data.
- The unlawful selling of personal data.
- The unlawful disclosure of personal data to unauthorised persons.

Further Information

Further information is available at www.informationcommissioner.gov.uk

Details of the Information Commissioner

The Information Commissioner's office is at:
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

Switchboard*:* 01625 545 700
Email: mail@ico.gsi.gov.uk
Data Protection Help Line: 01625 545 745
Notification Line: 01625 545 740

Revision History

Revision date	Summary of Changes	Other Comments
March 2019	Further details about breach and additional information about Cyber attacks	