Data Protection Policy

Introduction

Data protection is about ensuring people can trust organisations to use their data fairly and responsibly. The UK data protection regime is set out in the Data Protection Act 2018 along with the GDPR (General Data Protection Regulations) (which also forms part of UK law). The Information Commissioners Office (ICO) regulates data protection in the UK.

The following is not a definitive statement on the Act, but seeks to interpret relevant points where they affect Total Wellbeing Matters.

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

It is important to note that the Act covers all records relating to customers and staff

All Total Wellbeing Matters staff are required to follow this Data Protection Policy and Procedures at all times. Failure to do so may lead to disciplinary procedures.

The Managing Director has overall responsibility for data protection within Total Wellbeing Matters 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.
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. Total Wellbeing Matters is the Data Controller for the purposes of the Act.

Data Processor – an individual handling or processing data

Personal data – any information about a particular living individual which can identify who they are. This might be anyone, including a customer, customers, employee, partner, member, supporter, business contact, public official or member of the public.
Special categories of personal data – Some of the personal data processed can be more sensitive in nature and therefore requires a higher level of protection. The GDPR refers to the processing of these data as 'special categories of personal data'. This means personal data about an individual's:

- race
- ethnic origin

- political opinions,
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data
- health data
- sex life or sexual orientation

Data Protection Principles

Everyone responsible for using personal data must ensure that the information is:

- Used fairly, lawfully and transparently
- Used for specified, explicit purposes
- Used in a way that is adequate, relevant and limited to only what is necessary
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary
- Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

Individual's Rights

Under the Data Protection Act 2018 individuals have the right to find out what information Total Wellbeing Matters hold about them. These include the right to:

- Be informed about how data is being used
- Access personal data
- Have incorrect data updated
- Have data erased
- Stop or restrict the processing of their data
- Data portability (allowing the individual to get and reuse their data for different services)
- Object to how their data is processed in certain circumstances.

Procedures

Consent

Total Wellbeing Matters must record customers' explicit consent to storing certain information (known as 'personal data' or 'special categories of personal data') on file.

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

Total Wellbeing Matters will always seek written consent where personal 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 case remains open, retrospective consent should 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 Senior Management Team 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

Pro-forma should be used.

Telephone

Verbal consent should be sought and noted on the case record.

E-mail

The initial response should seek consent.

Consent obtained for one purpose cannot automatically be applied to all uses e.g., where consent has been obtained from a customer in relation to information needed for the provision of that service, separate consent would be required if, for example, a marketing letter was being mailed out.

Preliminary verbal consent should 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. 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 should be obtained in writing. Such media could be used for, but not limited to, publicity material, press releases, social media, and website. Consent should 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 should be sought.

Individuals have a right to withdraw consent at any time.

Ensuring the Security 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 customers for whom Total Wellbeing Matters hold personal details sign a consent form allowing us to hold such information.

   Customers may also consent for us to share personal or special categories of personal information with other helping agencies on a need-to-know basis. A customer's individual consent to share information should always be checked before disclosing personal information to another agency.

3. 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 Managing Director should first be sought.

4. Personal information should only be communicated within Total Wellbeing Matters' staff 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

Total Wellbeing Matters wishes to be an inclusive organisation. In order for Total Wellbeing Matters to monitor how well our staff, and customers reflect the diversity of the local community we request that they complete an Equality and Diversity Monitoring form. The completion of the form is voluntary, although strongly encouraged.

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 should 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/or special 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 customer's home, to the office for shredding this should 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 computers are networked, access to personal and special categories of personal information is restricted by password to authorised personnel only.

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.

If accessing emails, databases or other work-related data from a personal device such as mobile phone, tablet, laptop etc, you should ensure that adequate firewall and virus protection is installed at all times. You should also ensure that your device is password protected and that confidentiality is maintained so that others cannot have access to Total Wellbeing Matters data.

Privacy Statements

A Privacy Statement will also be published on our website explaining:

- Who we are
- What we will do with their data
- Who we will share it with
- Consent for marketing notice
- How long we will keep it for
- That their data will be treated securely
- How to opt out

.

All customers will receive a summary Privacy Notice when their consents are obtained. This Notice will explain what information we hold and why.

Staff will receive a detailed Privacy Notice upon appointment explaining the various pieces of information held and why.

Personnel Records

For staff who are regularly involved with vulnerable adults, it will be necessary for Total Wellbeing Matters to apply to the Disclosure & Barring Service (DBS) 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 Senior Management Team. If there is a positive disclosure the Managing Director will discuss this, anonymously, with our insurers to assess the risk of appointment. (Please refer to our Policy on the Disclosure & Barring Service.) Staff who are subject to DBS checks, must disclose any convictions, cautions, reprimands and final warnings which are issued to them after the DBS check has taken place. If there is a subsequent disclosure the Managing Director will discuss this, anonymously, with our insurers to assess the risk of continued appointment.

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 electronic data, e.g., documents and programmes related to work for Total Wellbeing Matters should not be stored on any external hard disk or on a personal computer. If documents need to be worked on at a non-networked device, they should be saved onto a USB drive which should be password protected or encrypted.

When sending emails or other electronic communications to outside organisations, e.g., social worker or hospital staff, care should be taken to ensure that any identifying data is removed and

that codes (e.g., initials or identifying code number, such as social services number, etc.) are to be used. Confidential and/or special categories of personal information should be written in a separate document which should be password protected before sending. Wherever possible, this document should be 'watermarked' confidential.

Any paperwork kept away from the office (e.g., customers care plan 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 (e.g., on a desktop) but kept in a file in a drawer or filing cabinet as examples, the optimum being a locked cabinet but safely out of sight is a minimum requirement. Staff needing to take paperwork away from a customer's home (e.g., unable to make a required phone call during the visit) must ensure that it is returned to the customer's home on the next visit.

If you are carrying documents relating to a number of customers when on a series of home visits, you should keep the documents for other customers locked out of sight in the boot of the car (not on the front seat) and not take them into the customers' home. When carrying paper files or documents they should be in a locked briefcase or in a folder or bag which can be securely closed or zipped up. The briefcase/folder/bag should contain Total Wellbeing Matters' 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 customer's home with the correct number of documents and that you haven't inadvertently left something behind.

Retention of Records

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

- Customers records – 6 years after ceasing to be a customer.
- Staff records – 6 years after ceasing to be a member of staff.
    - Staff pay records will be kept for three years as required by HMRC
- Unsuccessful staff application forms – 6 months after vacancy closing date.
- Timesheets and other financial documents – 7 years.
- Employer's liability insurance – 40 years.
- Other documentation, e.g., customers care plan sent to a worker as briefing for a visit, should be destroyed as soon as it is no longer needed for the task in hand.

Archived records should clearly display the destruction date.

What to Do If There Is a Breach

If you discover, or suspect, a data protection breach you should report this to the office who will review our systems to prevent a reoccurrence. The Managing Director should be informed of the breach, action taken and outcomes to determine whether it needs to be reported to the Information Commissioner. There is a time limit for reporting breaches to ICO so the Managing Director should be informed without delay.

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

Total Wellbeing Matters will not undertake direct telephone marketing activities under any circumstances.

Subject Access Requests (SARs)

Data Subjects can ask, in writing to the Managing Director, to see all personal data held on them, including e-mails and computer or paper files. The Data Processor (Total Wellbeing Matters) 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