Confidentiality & Data Protection

Having the correct data is vital in order that the Company can deliver effective support for all our Service Users. Personal data (any information which can identity an individual) belonging to Service Users and staff is one of our most valuable assets for the delivery of our service. This, together with the increasing reliance on IT to process and share information within the Company, creates a greater need to protect data processed within our systems

The Data Protection Act 2018 and UK GDPR sets out the legal framework by which we can process personal information safely and securely and operates alongside the common law duty of confidentiality which governs information given in confidence with the expectation that it will be kept confidential. The UK GDPR sets out seven data protection principles which describe legal requirements in relation to data processing. These principles are the key 'rules' for data handling and any processing of data which breaches one or more of the seven data protection principles is unlawful. As a data controller we are responsible for ensuring compliance with the UK GDPR, and we must be able to demonstrate our compliance. To comply with the principles of UK GDPR the Company must identify a lawful basis for processing the information, or the processing will be unlawful. The Company is required to register annually with the Information Commissioner's Office, which is the UK's independent body set up to uphold information rights. Our unique registration number is stored in The Business Continuity and Disaster Recovery Handbook

The DPA and the UK GDPR set out the legal requirements and duties placed on data controllers (the Company), and data processors (anyone we may use to process the data on our behalf) and explains the 'information rights' held by data subjects (people we hold information about). The policy will inform how the UK GDPR applies to the Company and our obligations. Under the UK GDPR each controller of personal information must decide what the lawful basis is for processing personal information. If there is no relevant basis, then the processing is likely to be illegal and regulatory action could be taken against the Company.

Key Principles:
As stated in the Data Protection Act 1998, personal data to be protected includes not only computer data but also certain manual and paper records. Employees have the right to receive a copy of personal data held on them on request and to demand that any inaccuracies are to be corrected or removed. They also have the right to be told whether and for what purpose personal information relating to them is being processed, the nature of the personal data and the people to whom the personal information may be disclosed. If this is required, the employee must submit a written request to the employer for this information

This company follows the eight basic principles contained within the Data Protection Act 1998:

1. Fair and lawful
   Personal data shall be processed fairly and lawfully and shall not be processed unless the data subject has given consent to the processing or unless the processing is absolutely necessary
2. Specific
   Personal data shall be obtained only for specified and lawful purposes and shall not be processed in any matter incompatible with these purposes
3. Adequate and relevant
   Personal data shall be adequate, relevant and not excessive. The personnel files of long-serving employees for example, may contain a backlog of out-of-date or irrelevant information. To guard against this, personnel files are periodically reviewed to ensure that there is a sound legal basis for continuing to hold the information
4. Accurate
   Personal data shall be accurate and kept up to date. To ensure this, once a year every employee and Service User shall be issued with a copy of their personnel files, giving them the opportunity to raise queries and notify us of any changes
5. Not kept for longer than necessary
   Personal data shall not be kept for longer than is necessary for the purpose it was processed. The personal information of service users who terminate their contract with us will be held on file for 1 year. Similarly, personnel files of ex-employees will be kept on file for 1 year before being destroyed

6. Individual Rights
   Personal data shall be processed in accordance with the rights of data subjects
7. Stored safely and securely
   Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data. Only authorized persons within the organization have access to data relating to clients or employees
8. Not transferred outside the EEA
   Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country ensures an adequate level of protection for the rights and freedoms of data subjects

Individual Rights

The UK GDPR provides enhanced rights for all individuals. These rights are mandated in the UK GDPR and Connect IoW CIC is required to act within a specific timeframe to any information request made to the Company

There are eight rights which all employees are required to be familiar with. These eight rights are:

1. The right to be informed - Individuals have the right to be informed about how their data is used, which is included in the Company's privacy notice
2. The right of access (Subject Access Request) - Individuals have the right ask for and receive a copy of their personal data
3. The right to rectification - Individuals have the right to have inaccurate personal data rectified or incomplete data to be completed
4. The right to erasure (Right to be forgotten) - Individuals have the right to ask for information to be erased; this is not an absolute right
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
6. The right to data portability - Allows individuals to obtain and reuse their personal data for their own purposes
7. The right to object - Individuals have the right to object to the processing of their personal data in certain circumstances
8. Rights in relation to automated decision-making and profiling - Where there is no human involvement in decision-making or profiling, this is restricted and can be challenged

As part of the UK GDPR's accountability principle we are required to safeguard individual rights by putting in place the appropriate technical and organisational measures. The UK GDPR requires the Company to integrate data protection into every aspect of our service. This includes implementation of the data protection principles and safeguarding individual rights, such as data minimisation, pseudonymisation and purpose limitation as set in this policy

Connect IoW CIC requires that data protection must be considered at the start of any new project, service, or process

It is Connect IoW CIC's policy:

1. To handle the information held about Service Users with confidentiality and respect
2. To ensure staff and Service Users are clear on the premise under which information will be shared with other professionals or involved persons/bodies
3. To ensure that where it is possible and lawful to do so, the Service User's permission will always be sought in the course of information sharing
4. To ensure that confidential information is held securely on behalf of the Service User and that access can be granted at any reasonable time

Procedure

Staff should:

1. Respect information about Service Users of their representatives that is confidential and handle such information in accordance with the Data Protection Act 1998 and UK GDPR
2. Take every possible precaution for the safe and confidential storage of Service User records and information

3. Always consult the Manager or Director if they are unclear with respect to any item concerning confidentiality
4. Ensure that any work-related paperwork that is no longer required is shredded at the earliest opportunity and not placed in a general waste basket
5. Ensure that tablets and phones are password/passcode protected

Staff should not:

1. Disclose confidential information to any unauthorised third party without express consent of the Service User, or if the Service User does not have capacity, the Service User's immediate family/carers
2. Seek confidential information from a Service User unless expressly in the interests of that Service User
3. Discuss any information pertaining to a service user or employee outside the Company or with any person not employed by the Company unless expressly authorized by the Director
4. Leave confidential information in an unsafe location (i.e. unattended)
5. Discuss a Service User in the presence of other Service Users

Policy: Personal Data Protection

The Company must operate within the Data Protection Act 1998 as holding personal data for 3 purposes:

1. Staff Administration
2. Accounts and Records
3. Health Administration and Services

All information held by the Company is strictly confidential. Written employment information is kept securely locked in the office. The Director, Company Secretary and Manager are the only people who have access to this information. Written private service user information is housed in the office and is only available to members of the Company

Any request made for personal data must be put in writing to the Director

Staff and service users will be required to annually approve a list of all personal data held pertaining to them. The maintaining and securing of this data is the responsibility of the Director

Data Breach

Any breach or suspected breach of data protection and confidentiality can have severe implications for the business, our Service Users and staff. Where significant numbers of individuals are involved, this can impact on the reputation of the Company as a whole

The Company is required to report serious breaches within 72 hours of the being made aware of the breach. GDPR requirements are for all organisations to report personal data breaches to the relevant supervisory authority, where the breach presents a risk to the affected individuals. The Director is the single point of contact for all breaches.

Staff must who wish to report incidents relating to data protection and confidentiality should follow the incident reporting procedures contained in the Reporting of Incidents Policy

Breaches of confidentiality or unauthorised disclosure of any information subject to the DPA and UK GDPR constitutes a serious disciplinary offence or gross misconduct under the Company's Disciplinary Policy. Staff found in breach of this policy may be subject to disciplinary action up to and including summary dismissal

For further information or advice concerning data protection and confidentiality, the Information Commissioners Office (ICO) should be contacted:

Email icocaseworker@ico.org.uk
Phone 0303 123 1113
Address Information Commissioner's Office
Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF

Policy last review date: 01.05.2024