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

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 sub-contractors.

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

The Managing Director has overall responsibility for data protection within the business but each individual processing data is acting on the company'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. The business 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 Business.

Data Protection Principles

As data controller, The Business 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
The Business must record service users' explicit consent to storing certain information (known as 'personal data' or 'special categories of personal data') on file.

For the purposes of the Regulations, personal and special categories of personal data covers information relating to:

1. The racial or ethnic origin of the Data Subject.
2. His/her political opinions.
3. His/her religious beliefs or other beliefs of a similar nature.
4. Whether he/she is a member of a trade union.
5. His/her physical or mental health or condition.
6. His/her sexual life.
7. The commission or alleged commission by him/her of any offence
8. Online identifiers such as an IP address
9. Name and contact details
10. Genetic and/or biometric data which can be used to identify an individual

Special categories of personal information collected by the Business will, in the main, relate to service users' physical and educational information. Data may 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 the Business will always seek 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 Managing Director 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, telephone and written - A pro-forma should be used.

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 service user in relation to information needed for the provision of that service, separate consent would be required if, for example, direct marketing of insurance products were to be undertaken.

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 in an email. 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

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.

4. A client's individual consent to share information should 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 Managing Director should first be sought.

6. Personal information should only be communicated by 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.

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 client's premises, 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.

Computer monitors in the reception area, or other public areas, should be positioned in such a way so that passers-by cannot see what is being displayed. If working in a public area, e.g. reception, you should 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.

Documents should only be stored on the server or cloud-based systems and not on individual computers.

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, the Business will satisfy themselves as to the compliance of data protection principles and robustness of the cloud-based providers.

Privacy Statements

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

- Explain 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
- Where they can find a copy of the full notice

Personnel Records

The Regulations apply equally to all staff records. The Business may at times record special categories of personal data as part of a staff member's contract of employment.

Confidentiality

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 the Business 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 computer they should be saved onto a USB drive which should be password protected.

Workstations in areas accessible to the public, e.g. reception or site, should 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, 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 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 client's office must ensure that it is returned to the client's office as soon as practically possible.

If you are carrying documents relating to a number of clients, you should keep the documents for other clients locked out of sight in the boot of the car (not on the front seat) and not take them into the client's office. 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 the Business 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 client's office 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:

- Client records – 6 years after ceasing to be a client.
- Staff records – 6 years after ceasing to be a member of staff.
- 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, should be destroyed as soon as it is no longer needed for the task in hand.

Archived records should clearly display the destruction date.

Computerised records, to be anonymised 10 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 should report this to your line manager who will review our systems, in conjunction with the Senior Management Team and our Quality Assurance & Systems Manager, to prevent a re-occurrence. The QA & Systems Manager 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 QA & Systems Manager 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.

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.
- Data cannot be used for the purposes of direct marketing of any goods or services if the Data Subject has declined their consent to do so.
- 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, the Business is permitted to store the personal data but not further process it. The Business 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'.

All Staff can request, (in writing to the Managing Director), to see all personal data held on them, including e-mails and computer or paper files. The Business 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