Data Protection and GDPR Policy for clients

Everyone has rights with regard to how their personal information is handled. During the course of our activities we will collect, store and process personal information about our clients and suppliers, and we recognise the need to treat it in an appropriate and lawful manner. We have a separate policy for the data of our employees.

The types of information that we may be required to handle include details of current, past and prospective suppliers, customers and others that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in The General Data Protection Regulation (GDPR).

This policy sets out how we seek to protect personal data and ensure that our staff and volunteers understand the rules governing their use of the personal data to which they have access during their work.

This policy requires staff to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed. They have overall responsibility for the day to day implementation of this policy.

Definition of Data Protection Terms

Data is information which is stored electronically, on a computer, or in certain paper-based filing systems.

Data subjects for the purpose of this policy include all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

Data controllers are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. We are the data controller of all personal data used in our business.

Data users include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

Data processors include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf.

Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

1. Data Protection Principles

Anyone processing personal data must comply with the eight enforceable principles of good practice. These provide that personal data must be:

1. Lawful, fair and transparent

Data collection must be fair, for a legal purpose and we must be open and transparent as to how the data will be used.

2. Limited for its purpose

Data can only be collected for a specific purpose.

3. Data minimisation

Any data collected must be necessary and not excessive for its purpose.

4. Accurate

The data we hold must be accurate and kept up to date.

5. Retention

We cannot store data longer than necessary.

6. Integrity and confidentiality

The data we hold must be kept safe and secure.

2. Fair and Lawful Processing

We must ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is (in this case it is us), the purpose for which the data is to be processed by us, and the identities of anyone to whom the data may be disclosed or transferred.

For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

3. Processing for Limited Purposes

Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected. This means that personal data must not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject must be informed of the new purpose before any processing occurs.

4. Data minimisation

Personal data should only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose should not be collected in the first place.

5. Accurate Data

Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and steps should therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data should be destroyed.

6. Retention

Personal data should not be kept longer than is necessary for the purpose. This means that data should be destroyed or erased from our systems when it is no longer required.

7. Integrity and confidentiality

We must ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data. Data subjects may apply to the courts for compensation if they have suffered damage from such a loss.

We must put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

I. **Confidentiality** means that only people who are authorised to use the data can access it.

II. **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.

III. **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

Security procedures include:

I. Any stranger seen in entry-controlled areas should be reported.

II. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)

III. Paper documents should be shredded. Computer hardware and related items should be appropriately wiped when they are no longer required.

IV. Data users should ensure that individual monitors do not show confidential information to passers-by and that they log off from their PC when it is left unattended.

V. Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords.

VI. Data stored on CDs or memory sticks must be encrypted or password protected and locked away securely when they are not being used

VII. The Data Protection Officer must approve any cloud used to store data

VIII. Data should be regularly backed up in line with the company's backup procedures

IX. Data should never be saved directly to mobile devices such as laptops, tablets or smartphones

X. All servers containing sensitive data must be approved and protected by security software

XI. All possible technical measures must be put in place to keep data secure

Dealing with Subject Access Requests:

Refer to privacy policy.

Providing Information over the Telephone:

Any member of staff dealing with telephone enquiries should be careful about disclosing any personal information held by us. In particular they should:

I. Check the caller's identity to make sure that information is only given to a person who is entitled to it.

II. Suggest that the caller put their request in writing if they are not sure about the caller's identity and where their identity cannot be checked.

Refer to the Chief Officer for assistance in difficult situations. No-one should be bullied into disclosing personal information

Reporting breaches

Any breach of this policy or of data protection laws must be reported as soon as practically possible. This means as soon as you have become aware of a breach. WYCAS has a legal obligation to report any data breaches to the Information Commissioner within 72 hours

All members of staff have an obligation to report actual or potential data protection compliance failures. This allows us to:

· Investigate the failure and take remedial steps if necessary
· Maintain a register of compliance failures
· Notify the [name of supervisory authority] of any compliance failures that are material either or as part of a pattern of failures

Any member of staff who fails to notify of a breach or is found to have known or suspected a breach has occurred but has not followed the correct reporting procedures will be liable to disciplinary action.

Please refer to our Chief Officer for our reporting procedure.

Failure to comply

We take compliance with this policy very seriously. Failure to comply puts both you and the organisation at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal.

Data Protection Officer is Simon Bostrom Finance Manager