Data Protection Policy

Policy Statement

Everyone has rights with regard to how their personal information is handled and this policy aims to respect those rights.

Safety and providing quality services is at the heart of everything we do, not just when we provide support services. It is very important to us that we keep all personal information that we hold safe and only use it in line with the data subject's wishes. We want them to be in control of their own data.

Data Protection legislation aims to prevent harm to those individuals we process data about by creating legal responsibility for keeping the information we hold as safe as possible. There are no secrets when it comes to how we use personal data and we only keep the information we need to help carry out our work.

The types of personal data that we may be required to handle relates to:-

- Employees
- Volunteers (including trustees)
- The People we support and their relatives and people who are looking for support
- Professionals (Local Authorities or health care professionals)
- Customers / suppliers and business contacts
- People who have a complaint about our services
- People who are interested in our work (marketing)
- Visitors to our website
- People who live in the properties that we own

The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in Data Protection Law which is in force at any given time ('the Law') and other regulations. The Law imposes restrictions on how we may use that information.

Status of the Policy

This policy sets out our rules on data protection and the legal conditions that must satisfy in relation to the personal information that we hold.

Our Data Protection Officer (DPO) is responsible for ensuring compliance with the Law and with this policy. Any questions or concerns about the operation of this policy should be referred in the first instance to our Data Protection Officer at dataprotectionofficer@avenuesgroup.org.uk.

Responsibilities

The Board / Company Directors	has overall responsibility for ensuring that the organisation complies with its legal obligations.
Data Protection Officer	Responsibilities include: • Briefing the Board on Data Protection responsibilities • Reviewing Data Protection and related policies • Advising other employees on tricky Data Protection issues • Ensuring that Data Protection induction and training takes place • Notification to the ICO • Handling subject access requests • Approving unusual or controversial disclosures of personal data • Approving contracts with Data Processors
Department Heads	monitoring their own compliance with this policy and reporting back to the DPO if they have any queries or concerns. Additional key responsibilities are outlined in the procedure.
Employees & Volunteers	All employees and volunteers are required to read, understand and accept any policies and procedures that relate to the personal data they may handle in the course of their work. (From now on, where 'employees' is used, this includes both paid employees and volunteers.)

Definitions

"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;

"Information Commissioners Office (ICO)" is the UK regulator of Data Protection Law;

"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;

"Special Category data" includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, genetic or biometric data, health information, sex life or sexual orientation, 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.

Data Protection Procedure

1. Data Protection Principles

1.1 Anyone processing personal data must comply with the six principles of Data Protection Law. These provide that personal data must be:

1.1.1 Principle 1: Personal data shall be processed lawfully, fairly and in a transparent manner;

1.1.2 Principle 2: Personal data should be collected for specific, explicit and legitimate reasons;

1.1.3 Principle 3: Personal data processing should be adequate, relevant and limited to only what is necessary;

1.1.4 Principle 4: Personal data should be accurate and where necessary kept up to date;

1.1.5 Principle 5: Personal Data should only be retained as long as is necessary;

1.1.6 Principle 6: Personal data should be processed in an appropriate manner to maintain security.

2. Principle 1: Personal data shall be processed lawfully, fairly and in a transparent manner

2.1 The first principle is aimed at making sure that the Data Subject knows exactly:

- who we are and how to contact us
- what we will be doing with their personal data
- how long we may need it
- why we are processing their personal data
- who we might share it with
- what their individual rights are

We do this in the form of a Privacy Policy which is on our website.

2.2 Upon collection of any personal information it is the employee's responsibility to ensure that the data subject is given access to our Privacy Policy which can be found on our website or in the form of a leaflet on MyAvenues.

2.3 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 special category 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. If you are unsure whether we are processing data lawfully you should seek advice or training from the Data Protection Officer.

2.4 The Law does not intend to prevent the use of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject.

3. Principle 2: Personal data should be collected for specific, explicit and legitimate reasons

3.1 Explicit, means that the Data Subjects must be able to choose which activities you can use their personal data for, and opt out of the activities they do not like. Legitimate means that if you can't justify the reason (legally) for collecting and using personal data; you should not be collecting it at all.

3.2 Personal data may only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. 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.

3.3 It is the responsibility of all employees to ensure that the Data Protection Officer is notified when we use data for a new purpose. The Data Protection Officer records this new purpose, identifies the legal basis for using the data and ensures it is in line with the Law. The Data Protection Officer is responsible for ensuring that the Privacy Policy is updated accordingly.

4. Principle 3: Personal data processing should be adequate, relevant and limited to only what is necessary

4.1 It is the responsibility of the employee who collects the personal data to make sure they only collect what we require for the purpose that it is being used. Any data which is not necessary for that purpose should not be collected in the first place.

5. Principle 4: Personal data should be accurate and where necessary kept up to date;

5.1 Personal data must be accurate and kept up to date. Information which is incorrect or misleading is not accurate and it is each department's responsibility to ensure that steps are 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 securely destroyed.

6. Principle 5: Personal Data should only be retained as long as is necessary;

6.1 Personal data should not be kept longer than is necessary for the purpose. This means that data should be securely destroyed or erased from our systems when it is no longer required and in line with our Data Retention and Confidential Waste Policies and Procedures.

6.2 It is each Line Managers responsibility to ensure that data is securely destroyed in line with the Data Retention Policy and that any changes to that policy are communicated immediately to the Data Protection Officer.

6.3 Many organisations keep a huge amount of data in databases or in archives, just in case. This principle means that if you no longer use the data in a process you should not have it.

7. Principle 6: Personal data should be processed in an appropriate manner to maintain security.

7.1 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.

7.2 The Act requires us to 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 there are necessary safeguards in place.

7.3 The Data Sharing Code of Practice issued by the ICO should always be considered along with the checklist before any personal information is shared. It is every employee's responsibility to ensure that this is done and that they Data Protection Officer is notified before any data is shared.

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

7.4.1 "Confidentiality "means that only people who are authorised to use the data can access it;

7.4.2 "Integrity" means that personal data must be accurate and suitable for the purpose for which it is processed;

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

7.5 Security procedures include:

7.5.1 "Entry controls" means any stranger seen in entry-controlled areas must be reported;

7.5.2 "Secure lockable desks and cupboards" means desks and cupboards must be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential);

7.5.3 "Methods of disposal" means paper documents must be shredded. Hard drives or external storage media (such as USB drives, external drives) and CD-ROMs must be physically destroyed when they are no longer required. All personal information must be destroyed in line with our Confidential Waste and Disposal Procedures;

7.5.4 "Equipment" means data users must ensure that individual monitors do not show confidential information to passers-by and that they log off, or lock their PC when it is left unattended in line with our Clear Desk and Secure Screen procedure;

7.5.5 "Password procedures" means passwords will be forced to expire at certain periods and passwords will need to be sufficiently complex in line with our Password Procedure;

7.5.6 "Encrypt data" means all personal data will be encrypted when it is in transit, including on portable devices in line with our Encryption Procedure;

7.5.7 "Monitor security logs" means failed attempts to log-in to our computer network will be monitored;

7.5.8 "User Accounts" means that ex employees user accounts are disabled on their departure of the organisation.

8. Individual Rights

8.1 Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the Law.

8.2 Data must be processed in line with data subjects' rights. Data subjects have a right to:

8.2.1 **be informed** about how we use their data. We do this by providing a privacy notice on our website and at the point of collecting their data. It is every employee's responsibility to ensure that people know about our Privacy Policy when collecting personal data.

8.2.2 have their personal data **corrected if it's inaccurate** and to have **incomplete personal data completed**. An individual can make a request verbally or in writing and we have one calendar month to respond. If a request is made the employee receiving the request should take reasonable steps to ensure that the data is accurate and rectify it if necessary. We can refuse to comply with a request for rectification if the request is excessive, taking into account whether the request is repetitive in nature. In this case you should contact the Data Protection Officer for assistance.

8.2.3 **object** to the processing of their personal data. This right only applies in certain circumstances.

8.2.4 **restrict the processing** of their personal data. An individual can make a request verbally or in writing and we have one calendar month to respond. This right only applies in the following circumstances:

- the individual contests the accuracy of their personal data and we are verifying the accuracy of the data;

- the data has been unlawfully processed (ie in breach of the lawfulness requirement of the first principle of the GDPR) and the individual opposes erasure and requests restriction instead;
- we no longer need the personal data but the individual needs us to keep it in order to establish, exercise or defend a legal claim; or
- the individual has objected to us processing their data under Article 21(1), and we are considering whether our legitimate grounds override those of the individual.

Any requests to restrict the processing of data should be sent to the Data Protection Officer immediately.

8.2.5 **have their personal data erased** (this is also known as the 'right to be forgotten'). An individual can make a request verbally or in writing and we have one calendar month to respond. This right only applies in the following circumstances:

- the personal data is no longer necessary for the purpose which we originally collected or processed it for;
- we are relying on consent as our lawful basis for holding the data, and the individual withdraws their consent;
- we are relying on legitimate interests as our basis for processing, the individual objects to the processing of their data, and there is no overriding legitimate interest to continue this processing;
- we are processing the personal data for direct marketing purposes and the individual objects to that processing;
- we have processed the personal data unlawfully (ie in breach of the lawfulness requirement of the 1st principle);
- we have to do it to comply with a legal obligation; or
- we have processed the personal data to offer information society services to a child.

Any requests to have data erased should be sent to the Data Protection Officer immediately.

8.2.6 **request access** to their personal data and information and more information about how we use it. This should be achieved in line with our Subject Access Request Policy. It is every employee's responsibility to read and be familiar with this policy.

8.2.7 **move, copy or transfer** your personal data (also know as 'data portability').

8.3 Data subjects also have the rights in relation to automated decision making including profiling.

8.4 If you receive a request relating to personal data and individual rights and you are unsure what you must do you must contact the Data Protection Officer for assistance without delay.

9. Dealing with Subject Access Requests

9.1 A formal request from a data subject for information that we hold about them must be made in writing and in line with our Subject Access Request Policy. It is the responsibility of any employee who receives a written request to forward it to their line manager or the Data Protection Officer immediately.

10. Providing Information over the Telephone

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

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

10.1.2 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; and

10.1.3 Refer to their line manager or the Data Protection Officer for assistance in difficult situations. No-one should be bullied into disclosing personal information.

11. Personal Data Breaches

11.1 A personal data breach can be defined as a security incident that has affected the confidentiality, integrity or availability of personal data.

11.2 It is the responsibility of all of our employees to contact our Data Protection Officer when a data breach takes place so that the Data Protection Officer can decide what action is required and if the breach has to be reported to the Information Commissioners Office (ICO).

11.3 It is our duty in Law to report certain types of personal data breach to the Information Commissioners Office (ICO). We must do this within 72 hours of becoming aware of the breach, where feasible.

11.4 If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, we must also inform those individuals without delay.

12. CCTV

12.1 Using CCTV can be privacy intrusive, as it is capable of putting a lot of law-abiding people under surveillance and recording their movements as they go about their day to day activities.

12.2 When using CCTV Avenues should carefully consider whether it is appropriate to use it; the fact that it is possible, affordable or has public support should not be the primary motivating factor. We should take into account what benefits can be gained, whether better solutions exist, and what effect it may have on individuals.

12.3 Any CCTV installation should only be implemented in line with the advice and guidance and only with a member of the Executive Management Team's prior approval.

13. Sending personal data outside of the UK and EEA

13.1 It is very unlikely that we will send personal data outside of the UK and the European Economic Area (EEA). However, there may be very rare occasions that we are required to do so (i.e. to respond to a reference request).

13.2 Countries inside the EEA and other 'safe countries' have adequate protections for personal data under laws similar to UK Law but in other countries steps will be taken to ensure appropriate safeguards are put in place so that data is protected before it is transferred.

13.3 If we have a need to transfer personal data outside of the UK/EEA or to an unsafe country we must ensure that it is done so in line with Data Protection Law.

12.4 It is every employee's responsibility to seek advice from the Data Protection Officer before transferring data outside of the UK / EEA unless it is deemed a safe country.