AGE Concern Petersfield and District

DATA PROTECTION AND GDPR POLICY

Contents

Purpose of the policy

Age Concern Petersfield & District is committed to complying with privacy and data protection laws including the General Data Protection Regulation ("**the GDPR**") and any related legislation which applies in the UK, including, without limitation, any legislation derived from the Data Protection Bill 2017; the Privacy and Electronic Communications Regulations (2003) and any successor or related legislation, including without limitation, E-Privacy Regulation 2017/0003; and all other applicable laws and regulations relating to the processing of personal data and privacy, including statutory instruments and, where applicable, the guidance and codes of practice issued by the Information Commissioner's Office ("ICO") or any other supervisory

authority. (together "**the Legislation**")

This policy sets out what we do to protect individuals' personal data.

Anyone who handles personal data in any way on behalf of Age Concern Petersfield & District must ensure that we comply with this policy. Section 3 of this policy describes what comes within the definition of "personal data". Any breach of this policy will be taken seriously and may result in disciplinary action or more serious sanctions.

This policy may be amended from time to time to reflect any changes in Legislation, regulatory guidance or internal policy decisions.

The types of personal data that we handle include details of:

Staff, Volunteers, Service Providers, Service Users, Residents, Health and Social Care Professionals, Council contacts. It is important for Age Concern Petersfield & District to share this information in relation to the running of our services and to enable us to conduct the business of the charity.

All Employees and Volunteers sign an agreement (as part of their application form) to treat any information given to them as highly confidential. The storage of such data is explained within this policy.

Definitions of data protection terms

The following terms will be used in this policy and are defined below:

Data Subjects include all individuals about whom we hold personal data, for instance an employee or a supporter. 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 any information relating to a person who can be identified directly or indirectly from that information (or from that information 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). It can also include an identifier such as identification number, location data, an online identifier specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

Data Controllers are the people who, or organisations which, decide the purposes and the means for which, any personal data is processed. They have a responsibility to process personal data in compliance with the Legislation. Age Concern Petersfield & District is the data controller of all personal data that we manage in connection with our work and activities.

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 other organisations such as website hosts, fulfilment houses or other service providers which handle personal data on our behalf.

European Economic Area includes all countries in the European Union as well as Norway, Iceland and Liechtenstein.

ICO means the Information Commissioner's Office (the authority which oversees data protection regulation in the UK).

Processing is any activity that involves use of personal data, whether or not by automated means. It includes but is not limited to:

a. collecting;
b. recording;
c. organising;
d. structuring;
e. storing;
f. adapting or altering;
g. retrieving;
h. disclosing by transmission;
i. disseminating or otherwise making available;
j. alignment or combination;
k. restricting;
l. erasing; or
m. destruction of personal data.

Sensitive Personal Data (which is defined as "special categories of personal data" under the GDPR) includes information about a person's:

a. racial or ethnic origin;
b. political opinions;
c. religious, philosophical or similar beliefs;
d. trade union membership;
e. physical or mental health or condition;
f. sexual life or orientation;
g. genetic data;
h. biometric data; and
i. such other categories of personal data as may be designated a "special categories of personal data" under the Legislation.

Data protection principles. Anyone processing personal data must comply with the six data protection principles set out in the GDPR. We are required to comply with these principles (summarised below), and show that we comply, in respect of any personal data that we deal with as a data controller.

Personal data should be:

a) processed fairly, lawfully and transparently;

b) collected for specified, explicit and legitimate purposes and not further processed in a way which is incompatible with those purposes.

c) adequate, relevant and limited to what is necessary for the purpose for which it is held accurate and, where necessary, kept up to date;

d) not kept longer than necessary; and

e) processed in a manner that ensures appropriate security of the personal data.

Processing data fairly and lawfully

First Data Protection Principle – Personal data must be obtained fairly and lawfully and processed for purposes that the data subject has been told about. Processing will only be lawful if certain conditions can be satisfied, including where the data subject has given consent, or where the processing is necessary for one or more specified reasons, such as where it is necessary for the performance of a contract.

To comply with this principle, every time we receive personal data about a person directly from that individual, which we intend to keep, we need to provide that person with "**the fair processing information**". In other words we need to tell them:

A. the type of information we will be collecting (categories of personal data concerned);
B. who will be holding their information, i.e. Age Concern Petersfield & District including contact details and the contact details of our Data Protection Officer (if we have one);
C. why we are collecting their information and what we intend to do with it for instance to process donations or send them mailing updates about our activities;
D. the legal basis for collecting their information (for example, are we relying on their consent, or on our legitimate interests or on another legal basis);
E. if we are relying on legitimate interests as a basis for processing what those legitimate interests are;
F. whether the provision of their personal data is part of a statutory or contractual obligation and details of the consequences of the data subject not providing that data;
G. the period for which their personal data will be stored or, where that is not possible, the criteria that will be used to decide that period;
H. h) details of people or organisations with whom we will be sharing their personal data;
I. if relevant, the fact that we will be transferring their personal data outside the EEA
J. and details of relevant safeguards; and the existence of any automated decision-making including profiling in relation to that personal data.

Where we obtain personal data about a person from a source other than the person his or her self, we must provide that individual with the following information:-

a) the categories of personal data that we hold; and

b) the source of the personal data and whether this is a public source.

In addition, in both scenarios, (where personal data is obtained both directly and In-directly) we must also inform individuals of their rights including the right to lodge a complaint with the ICO and, the right to withdraw consent to the processing of their personal data.

This fair processing information can be provided in a number of places including on web pages, in mailings or on application forms. We must ensure that the fair processing information is concise, transparent, intelligible and easily accessible.

Processing data for the original purpose

Second Data Protection Principle requires that personal data is only processed for the specific, explicit and legitimate purposes that the individual was told about when we first obtained their information.

This means that we should not collect personal data for one purpose and then use it for another. If it becomes necessary to process a person's information for a new purpose, the individual should be informed of the new purpose beforehand. For example, if we collect personal data such as a contact number or email address, in order to update a person about our activities it should not then be used for any new purpose, for example to share with other organisations for marketing purposes, without first getting the individual's consent.

Personal data should be adequate and accurate

Third and Fourth Data Protection Principles require that personal data that we keep should be accurate, adequate and relevant. Data should be limited to what is necessary in relation to the purposes for which it is processed. Inaccurate or out-of date data should be destroyed securely, and we must take every reasonable step to ensure that personal data which is inaccurate is corrected.

Not retaining data longer than necessary

Fifth Data Protection Principle requires that we should not keep personal data for longer than we need to for the purpose it was collected for. This means that the personal data that we hold should be destroyed or erased from our systems when it is no longer needed. Processes for shredding and deletion of data on IT devices and deletion of data in the event of IT hardware being disposed of are stringently followed.

If you think that we are holding out-of-date or inaccurate personal data, please contact the office of Age Concern Petersfield & District.

Rights of individuals under the GDPR

The GDPR gives people rights in relation to how organisations process their personal data.

Everyone who holds personal data on behalf of Age Concern Petersfield & District needs to be aware of these rights. They include (but are not limited to) the right:

a) to request a copy of any personal data that we hold about them (as data controller), as well as a description of the type of information that we are processing, the uses that are being made of the information, details of anyone to whom their personal data has been disclosed, and how long the data will be stored (known as subject access rights);

b) to be told, where any information is not collected from the person directly, any available information as to the source of the information;

c) to object to the processing of data where the processing is based on either the conditions of public interest or legitimate interests;

d) to have all personal data erased (the right to be forgotten) unless certain limited conditions apply;

e) to restrict processing where the individual has objected to the processing;

f) to have inaccurate data amended or destroyed; and

g) to prevent processing that is likely to cause unwarranted substantial damage or distress to themselves or anyone else.

Data Protection Security

Sixth Data Protection Principle requires that we keep secure any personal data that we hold.

We are required to put in place procedures to keep the personal data that we hold secure, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

When we are dealing with sensitive personal data, more rigorous security measures are likely to be needed, for instance, if sensitive personal data (such as details of an individual's health, race or sexuality) is held on a memory stick or other portable device it should always be encrypted.

When deciding what level of security is needed, your starting point should be to look at whether the information is sensitive or highly confidential and how much damage could be caused if it fell into the wrong hands.

The following security procedures and monitoring processes must be followed in

relation to all personal data processed by us: encryption of personal data; measures to restore availability and access to data in a timely manner in event of physical or technical incident; process for regularly testing, assessing and evaluating effectiveness of security measures; backing up data (daily back-ups should be taken of all data on the system and data should not be stored on local drives or removable media as these will not be backed up); entry controls (any stranger seen in entry controlled areas should be reported); staff 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; paper documents should be shredded, memory sticks, CD ROMs and other media on which personal data is stored should be physically destroyed when they are no longer required; personal data must always be transferred in a secure manner (the degree of security required will depend on the nature of the data - the more sensitive and confidential the data, the more stringent the security measures should be) other measures to ensure confidentiality, integrity, availability and resilience of processing systems; desks and cupboards should be kept locked if they hold confidential information of any kind (personal information is always considered confidential) and staff must keep data secure when travelling or using it outside the offices.

Transferring Data Outside the EEA - The GDPR requires that when organisations transfer personal data outside the EEA, they take steps to ensure that the data is properly protected. The European Commission has determined that certain countries provide an adequate data protection regime. In the event that this process is a possibility (which may be via grant funding requirements) please ensure the relevant checks are made to ensure compliance.

Processing sensitive personal data – On some occasions we may collect information about individuals that is defined by the GDPR as **special categories of personal data**, and special rules will apply to the processing of this data. In this policy we refer to “special categories of personal data” as “sensitive personal data”.

Purely financial information is not technically defined as sensitive personal data by the GDPR. However, particular care should be taken when processing such data, as the ICO will treat a breach relating to financial data very seriously.

In most cases, in order to process sensitive personal data, we must obtain explicit consent from the individuals involved. As with any other type of information we will also have to be absolutely clear with people about how we are going to use their information.

It is not always necessary to obtain explicit consent. There are a limited number of other circumstances in which the GDPR permits organisations to process sensitive personal data. If you are concerned that you are processing sensitive personal data and are not able to obtain explicit consent for the processing, please contact the office of Age Concern Petersfield & District.

Notification

We recognise that whilst there is no obligation for us to make an annual notification to the ICO under the GDPR, we will consult with the ICO where necessary when we are carrying out “high risk” processing.

We will report breaches (other than those which are unlikely to be a risk to individuals) to the ICO where necessary, as a matter of urgency. We will also notify affected individuals where the breach is likely to result in a high risk to the rights and freedoms of these individuals.

Monitoring and review of the policy

This policy is reviewed regularly by our Board of Trustees, or additionally at times there may be changes to the governing rules and regulations for Data Protection and GDPR to ensure that it is achieving its objectives.

The Board of Trustees at Age Concern Petersfield & District hold the overall responsibility for ensuring compliance with Data Protection and GDPR requirements. Any question, queries or concerns about this policy should be referred in the first instance to Mrs Rosemary Bishop, Chair of the Board of Trustees, Age Concern Petersfield & District c/o Winton House, 18 High Street, Petersfield, Hampshire GU32 3JL. info@ageconcernpetersfield.org.uk

POLICY STATEMENT

All Policies and Procedures held by Age Concern Petersfield & District are regularly reviewed and may be amended from time to time to reflect any changes in Legislation, regulatory guidance or internal policy decisions, as well as for any other reasons determined by the Board of Trustees. The latest versions will always be reflected on our website.