CITIZENS ADVICE REIGATE AND BANSTEAD DATA PROTECTION POLICY

1. Statement of policy

Citizens Advice Reigate and Banstead is fully committed to compliance with the requirements of the General Data Protection Regulation (GDPR), Data Protection Act 2018 and any successor legislation (together, the 'data protection legislation'). Citizens Advice Reigate and Banstead is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal data and special category personal data.

Citizens Advice Reigate and Banstead will therefore follow procedures which aim to ensure that all employees and volunteers, and others who have access to any personal data held by or on behalf of the local office, are fully aware of and responsible for the handling of personal data in line with the data protection legislation.

In order to operate efficiently, Citizens Advice Reigate and Banstead has to collect and use information about people with whom it works. These may include current, past and prospective clients; current, past and prospective employees; current, past and prospective volunteers; and our suppliers.

2. Use of personal data

Data protection legislation and in particular Article 5 (1) of the GDPR requires that personal data shall be used in accordance with the following principles:

a) processed lawfully, fairly and in a transparent manner in relation to individuals;

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

Article 5 (2) of the GDPR requires that:

“the controller shall be responsible for, and be able to demonstrate, compliance with the principles.”

3. Lawful basis for processing personal data under the data protection legislation
Article 6 of the GDPR sets out six lawful bases for processing data:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/

At least one of these must apply whenever personal data is processed:

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone’s life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests.

Citizens Advice Reigate and Banstead primarily use legitimate interest to process client personal data but may also process personal data under the other 5 lawful bases following lawful bases set out above.

4. Lawful basis for processing special category personal data
In order to lawfully process special category data, you must identify both a lawful basis under GDPR: Article 6 and a separate condition for processing special category data under GDPR: Article 9. These do not have to be linked.

There are ten conditions (GDPR: Article 9(2)) for processing special category data in the GDPR itself, but the Data Protection Act 2018 introduces additional conditions and safeguards.
You need to read these alongside the Data Protection Act 2018, which adds more specific conditions and safeguards:

Schedule 1 Part 1 contains specific conditions for the various employment, health and research purposes under Articles 9(2)(b), (h), (i) and (j).
Schedule 1 Part 2 contains specific ‘substantial public interest’ conditions for Article 9(2)(g).
In some cases you must also have an ‘appropriate policy document’ in place to rely on these conditions.

You must determine your condition for processing special category data before you begin this processing under the GDPR and you should document it.

Link to Article 9(2)GDPR 10 conditions for processing special category data:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

The conditions are listed in Article 9(2) of the GDPR:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Citizens Advice Reigate and Banstead process special category personal data under the following lawful bases:

Explicit consent: the data subject has given explicit consent to the processing of those personal data for one or more specified purposes.

5. Handling of personal data and special category personal data

Citizens Advice Reigate and Banstead will, through appropriate management and the use of appropriate controls adhere to the following in regards to our use of personal data and special category personal data;

- Provide up to data privacy notices to data subjects.
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with legal requirements.
- Ensure the quality and accuracy of information when collected or received and during its use.
- Apply checks to determine the length of time information is retained.
- Take appropriate technical and organisational security measures based on risks to data subjects.
- Not transfer outside the EEA without suitable safeguards.
- Ensure that any information incidents are reported to national Citizens Advice and where appropriate the data subject and the Information Commissioners Office.
- Mitigate risks to the data subjects in the event of an information incident using an appropriate data breach policy.
- Ensure that the rights of our data subjects can be properly exercised.

These rights include:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erase
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

In addition, we will ensure that:

- There is someone with specific responsibility for data protection in the organisation. The post responsible for data protection is the Advice Services Manager

- Organisational information and in particular privacy risks are risk assessed, documented and controlled.

- Everyone managing and handling personal data and special category personal data understands that they are responsible for following good Information

- Governance/Assurance practice and for complying with the data protection legislation.

- Everyone managing and handling personal data and special category personal data is appropriately trained and supervised to do so.

- Queries about processing personal data and special category personal data are promptly and courteously dealt with within the requirements of the data protection legislation.

- Data sharing and processing is carried out under an appropriate written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

All employees and volunteers are to be made fully aware of this policy and their duties and responsibilities under it. All employees and volunteers will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure.

6. Client management systems

As part of our membership of CitA, Citizens Advice Reigate and Banstead will use the relevant case management system provided by CitA, (currently Casebook) and by doing so agrees to adhere to the data sharing agreement between the respective parties.

CitA and Citizens Advice Reigate and Banstead are joint data controllers for the personal data and special category personal data within the Casebook application and therefore each have a joint responsibility to ensure compliance with data protection legislation.

Casebook is used to process information, personal data and special category personal data provided by clients in the course of seeking advice and guidance from the CitA.

All information, personal data and special category personal data is to be regarded as being confidential between the individual and the Citizens Advice service unless expressly indicated otherwise.

Data sharing is required so that both the client and CitA have flexibility in where, how and when clients receive the service and the need to only enter this client data once. The data protection legislation provides the legal framework under which personal data and special category personal data can be processed.

Data is shared to provide the service to clients, to refer clients to other organisations, for following up with the client for feedback, to enable CitA to act on behalf of the client when authorised, to understand trends and carry out research to enable policy work. The data shared will always be the minimum necessary required to carry out the business purpose.

In all cases the relevant consent must be obtained, or alternative lawful basis determined, for any processing or sharing of client personal data and special category personal data.

7. Relationship with existing policies and supporting documentation

This policy has been formulated within the context of a range of policies such as those relating to IT security, confidentiality and information assurance.