DATA PROTECTION & INFORMATION SECURITY POLICY

1. Statement of Policy

North East Suffolk Citizens Advice Bureau 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 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.

North East Suffolk Citizens Advice Bureau 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, North East Suffolk Citizens Advice Bureau 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.

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."

Lawful basis for processing personal data and special category persona data under the data protection legislation

North East Suffolk Citizens Advice Bureau primarily uses legitimate interest to process client personal data. 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. Personal data may also be processed on other lawful grounds or a combination of lawful grounds. Another example is explicit consent: the data subject has given explicit consent to the processing of those personal data for one or more specified purposes.

2. Handling of personal data and special category personal data

North East Suffolk Citizens Advice Bureau 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 Commissioner's 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 Senior Information Risk Officer currently Janet John.
- 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.

3. Client management systems

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

Citizens Advice and each individual local Citizens Advice 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 Citizens Advice service.

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 Citizens Advice 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 Citizens Advice 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.

4. Training

All employees and volunteers will undertake data protection and information security training on an annual basis or more frequently if necessary. Training records will be kept for each individual.

5. Breaches and Compliance

Any data security incidents must immediately be reported to the Senior Information Risk Officer who will without delay contact the National Citizens Advice Operations Team and complete the online incident form as directed by them. A copy of the completed form will be retained in a central file.

Any breach of the terms of this policy will be considered seriously and may result in disciplinary or equivalent volunteer proceedings which in some cases may be considered gross misconduct. Some instances may also constitute a criminal offence.

6. 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 and should be read in conjunction with those polices. All policies are subject to review on an annual basis or more frequently if necessary.

7. Appendices

A: "How to keep client's personal information safe" leaflet