



East Herts Citizens Advice Service

DATA PROTECTION POLICY

East Herts Citizens Advice Service (EHCAS) is fully committed to compliance with the requirements of the Data Protection Act 1998 which came into force on 1 March 2000.

EHCAS will therefore follow procedures which aim to ensure that anyone who has access to any personal data held by or on behalf of the bureau, are fully aware of and abide by their duties under the Data Protection Act 1998.

EHCAS is committed to a policy of protecting the rights and freedoms of individuals with respect to the processing of their personal data.

1. Statement of Policy

In order to operate efficiently, EHCAS has to collect and use information about people with whom it works. These may include clients; current, past and prospective staff; past and prospective volunteers; and suppliers. In addition, it may be required by law to collect and use information in order to comply with the requirements of central government.

This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means, and there are safeguards within the Act to ensure this.

Given the nature of the service and its aims and principles, EHCAS views the lawful and correct treatment of personal information as very important to its successful operations, and to maintaining confidence between bureaux and those with whom they carry out business.

To this end, EHCAS fully endorses and adheres to the principles of data protection as set out in the Data Protection Act 1998.

2. The Eight Principles of Data Protection

The Act stipulates that anyone processing personal data must comply with eight principles of good practice. These principles are legally enforceable.

Schedule 1 to the Data Protection Act lists the eight principles in the following terms:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

- (a) at least one of the conditions in Schedule 2 is met (see below), and
- (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met (see also below).
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
 3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
 4. Personal data shall be accurate and, where necessary, kept up to date.
 5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
 6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
 7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
 8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

To comply with Schedule 2 and Schedule 3 of the Data Protection Act in practise, EHCAS must:

- have legitimate grounds for collecting and using the personal data;
- not use the data in ways that have unjustified adverse effects on the individuals concerned;
- be transparent about how the data will be used, and give individuals appropriate privacy notices when collecting their personal data;
- handle people's personal data only in ways they would reasonably expect; and
- make sure nothing unlawful is done with the data.

3. Personal Data and “Sensitive” Personal Data

The Act makes a distinction between personal data and “sensitive” personal data.

Personal data means data which relates to a living individual who can be identified -

- from that data, or
- from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller,

and includes an expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.



Sensitive personal data means personal data consisting of information as to:

- (a) the racial or ethnic origin of the data subject,
- (b) his political opinions
- (c) his religious beliefs or other beliefs of a similar nature,
- (d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992),
- (e) his physical or mental health or condition,
- (f) his sexual life,
- (g) the commission or alleged commission by him of any offence, or
- (h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

4. Handling of Personal Data and Sensitive Personal Data

EHCAS will, through appropriate management and the use of strict criteria and controls:-

- Observe fully conditions regarding the fair collection and use of personal information
- Meet its legal obligations to specify the purpose for which information is used
- Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements
- Ensure the quality of information used
- Apply checks to determine the length of time information is held
- Take appropriate technical and organisational security measures to safeguard personal information
- Ensure that personal information is not transferred abroad without suitable safeguards
- Ensure that the rights of people about whom the information is held can be fully exercised under the Act.

These include:

- The right to be informed that processing is being undertaken.
- The right of access to one's personal information within the statutory 40 days.
- The right to prevent processing in certain circumstances.
- The right to correct, rectify, block or erase information regarded as wrong information.

In addition, EHCAS will ensure that:

- There is someone with specific responsibility for data protection in the bureau



- Everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice
- Everyone managing and handling personal information is appropriately trained to do so
- Everyone managing and handling personal information is appropriately supervised
- Anyone wanting to make enquiries about handling personal information, whether a member of staff or volunteer or a member of the public, knows what to do
- Queries about handling personal information are promptly and courteously dealt with
- Methods of handling personal information are regularly assessed and evaluated
- Performance with handling personal information is regularly assessed and evaluated
- Data sharing is carried out under a written agreement, setting out the scope and limits of the sharing. Any disclosure of personal data will be in compliance with approved procedures.

All staff and volunteers are to be made fully aware of this policy and of their duties and responsibilities, and will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure. In particular they will ensure that:

- Paper files and other records or documents containing personal / sensitive data are kept in a secure environment
- Personal data held on computers and computer systems is protected by the use of secure passwords
- Individual passwords are such that they are not easily compromised.

5. Use of Case

EHCAS uses CASE to electronically record the advice given to clients.

CASE facilitates adherence to the Data Protection Act as it has a 'check box' to allow EHCAS to enter the fact that consent has been obtained. This 'check box' can be updated on every contact.

The CASE servers (for data storage and application access) are hosted at the Logica Data Centre in Bridgend, South Wales. The data centre is designed specifically to host data and applications for many clients, and therefore are secured both physically and electronically. The environment, security policy and procedure for the CASE application are based on ISO 27001, as recommended by the Information Commissioner's office.

Security systems in bureaux are subject to guidelines issued from Citizens Advice.

The connection between the individual bureaux and the CASE hosting environment is via a secure private network based on telecommunications links from a central hub at the



hosting centre to each bureau. All relevant parties (HP, Logica, Azzurri, and Citizens Advice) have been checked for appropriate notification.

6. Implementation

The Manager is responsible for leading and monitoring policy implementation. They will also have overall responsibility for:

- the provision of cascade data protection training for staff and volunteers within the bureau
- carrying out compliance checks to ensure adherence, throughout the bureau, with the Data Protection Act.

7. Notification to the Information Commissioner

The Information Commissioner maintains a public register of data controllers. East Herts Citizens Advice Service is registered as such.

The Data Protection Act 1998 requires every data controller who is processing personal data to notify and renew their notification on an annual basis. Failure to do so is a criminal offence.

The manager will review the Data Protection Register annually, prior to notification to the Information Commissioner.

Any changes to the register must be notified to the Information Commissioner within 28 days. To this end, any changes made between reviews will be brought to the attention of the Director of Corporate Affairs immediately.

8. Relationship with Existing Policies and Supporting Documentation

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

In addition, pro formas are in use for requesting consent to store data (from clients, staff and volunteers).