Data Protection Policy

Updated October 2016

Data Protection Policy

Introduction

Huntingdonshire District Council is fully committed to compliance with the requirements of the Data Protection Act 1998 ("the Act"), which came into force on the 1st March 2000 and with Article 8 of the Human Rights Act 1998. Both Acts stress that the processing of personal data needs to strike a balance between, on the one hand, the needs of the organisation to function effectively and efficiently and, on the other, respect for the rights and freedoms of the individual.

The Council will therefore follow procedures that aim to ensure that all employees, elected members, contractors, agents, consultants, partners or other servants of the council who have access to any personal data held by or on behalf of the council, are fully aware of and abide by their duties and responsibilities under the Act.

Statement of policy

In order to operate efficiently, the council has to collect and use information about people with whom it works. These may include members of the public, current, past and prospective employees, clients and customers, 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.

The council regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the council and those with whom it carries out business. The council will ensure that it treats personal information lawfully and correctly.

To this end the council fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 1998.

The 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.

The Principles require that personal information:

1. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met;
2. 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. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
4. Shall be accurate and where necessary, kept up to date;
5. Shall not be kept for longer than is necessary for that purpose or those purposes;
6. Shall be processed in accordance with the rights of data subjects under the Act;
7. Shall be kept secure i.e. protected by an appropriate degree of security;
8. Shall not be transferred to a country or territory outside the European

Economic Area, unless that country or territory ensures an adequate level of data protection.

The Act provides conditions for the processing of any personal data. It also makes a distinction between **personal data and "sensitive" personal data**.

Personal data is defined as, data relating to a living individual who can be identified from:

- That data;
- 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 is defined as personal data consisting of information as to:

- Racial or ethnic origin;
- Political opinion;
- Religious or other beliefs;
- Trade union membership;
- Physical or mental health or condition;
- Sexual life;
- Criminal proceedings or convictions.

Handling of personal/sensitive information

Huntingdonshire District Council will, through appropriate management and the use of strict criteria and controls:-

- Observe fully conditions regarding the fair collection and use of personal information, see Appendix A;
- 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 strict 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, Huntingdonshire District Council will ensure that:

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

- 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 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 elected members are to be made fully aware of this policy and of their duties and responsibilities under the Act.

All managers and staff within the council's directorates will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and in particular 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, which where possible have forced changes periodically;
- Individual passwords should be such that they are not easily compromised.

All contractors, consultants, partners or other servants or agents of the Council must:

- Ensure that they and all of their staff who have access to personal data held or processed for or on behalf of the council, are aware of this policy and are fully trained in and are aware of their duties and responsibilities under the Act. Any breach of any provision of the Act will be deemed as being a breach of any contract between the council and that individual, company, partner or firm;
- Allow data protection audits by the council of data held on its behalf (if requested);
- Indemnify the council against any prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

All contractors who are users of personal information supplied by the council will be required to confirm that they will abide by the requirements of the Act with regard to information supplied by the council.

Implementation

The council has appointed a Data Protection Officer. Designated officers have also been identified in all directorates. These officers will be responsible for ensuring that the Policy is implemented. Implementation will be led and monitored by the Information Officer. The Information Officer will also have overall responsibility for:

- The provision of data protection training, for staff within the council.
- For the development of best practice guidelines.
- For carrying out compliance checks to ensure adherence, throughout the authority, with the Data Protection Act.

Subject Access and Subject Information Requests

All data subjects whose details are held/processed by the Council have a general right to receive copies of their own information. There are some exceptions, for example, data held for child protection or crime detection or where information cannot be given without reference to a third party unless that third party has given his or her consent.

The Data Protection Officer will be responsible to decide whether data held is exempt from disclosure.

A request for access or information must be made using the appropriate form to ensure sufficient details to enable the Council to conduct a data search in order to fulfil the request. The request should be addressed to the Data Protection Officer, or in his absence, the Head of Legal and Democratic Services. No other employee will be permitted to receive or process access or information requests. A charge of £10.00 is payable (reviewable from time to time by the Head of Legal & Democratic Services but such fee will not exceed the Prescribed Maximum as set out in the Act).

The Council will respond to subject access or information requests as soon as possible and in all cases within 40 days of the request. In some cases, especially where requests are not submitted on the correct form, further information may be required which may delay the start of the 40 day maximum period.

The Data Protection Officer will refuse repeated requests where such requests are received so soon after the previous request that it would be impossible for the details to have changed or in other cases where the Data Protection Officer in consultation with the Head of Legal and Democratic Services deem the request unreasonable.

Notification to the Information Commissioner

The Information Commissioner maintains a public register of data controllers. Huntingdonshire District Council 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.

To this end the designated officers will be responsible for notifying and updating the Information Officer of the processing of personal data, within their directorate.

The Information Officer will review the Data Protection Register with designated officers 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 Information Officer immediately.

Further Information Enquires and Complaints

The Council's Data Protection Officer is the first point of contact on any of the matters raised in this policy statement. Enquiries should be addressed to:

The Data Protection Officer
Huntingdonshire District Council
Pathfinder House
St. Mary's Street
Huntingdon
Cambridgeshire
PE29 3TN

Email: data.protection@huntingdonshire.gov.uk

The Data Protection Officer will be responsible for dealing with all internal and external complaints. All complaints should be in writing, dated and include details of the complaint and also an account of the nature of the problem.

The Council will attempt to complete any internal investigations within 20 working days. An acknowledgement of the complaint should be dispatched to the complainant as soon as practicable after its receipt.

Updated October 2016

Appendix A:

Fair Obtaining and Processing of Personal Data

The Council will, so far as practicable, ensure that no manual or automatic processing shall take place unless reasonable steps have been taken to make the data subject aware of that processing.

In addition data subjects will, where possible, be informed of the likely recipients of the information (internal or external to the Council).

Processing of personal data within the Council will be fair and lawful and data subjects will not be misled as to the uses to which the Council will put the personal data. A complaints procedure for data subjects who consider they have been deceived or misled appears on page 6 of this policy statement.

Any forms requiring personal data should contain a statement by the Council giving details of the proposed uses of the information and where information is collected in person or by telephone, the employee asking for personal data will tell the data subject how the personal data will be used. Data subjects are free to ask the person collecting the information why they want the data and what they are used for.

If personal data is to be used for auto-decision making (where a computer decides something based on a score or other information) the person will be told how the system works and whether the decisions can be challenged.

Any person whose details are to be included in the Council's web site will be asked to give their written consent and informed about the possible consequences of their data being disseminated world-wide.