HERTSMERE BOROUGH COUNCIL

DATA PROTECTION POLICY

October 2007

1. Introduction

Hertsmere Borough Council ('the Council') is fully committed to compliance with the requirements of the Data Protection Act 1998 ('the Act'), which came into force on the 1 March 2000. The Act sets out rules for processing personal information (known as personal data) and applies to all personal data that is processed automatically, any personal data held in a manual form in a relevant filing system and any personal data held in an accessible record.

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.

This policy sets out the Council's approach to data protection and compliance with good information handling practice. This covers the whole lifecycle, including:

- Obtaining of personal data
- The storage and security of personal data
- The use of personal data
- The disposal / destruction of personal data.

2. Statement of Intent

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, 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. Any employee found to be deliberately acting outside their authority will be subject to the Council's disciplinary procedure.

To this end the Council fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 1998 and will update or amend this policy as necessary according to the laws of England and Wales.

3. Definitions

To aid the understanding of this policy and the provisions of the Data Protection Act, the following definitions are provided:

Personal data – data which relate to a living individual who can be identified from those data or any other data likely to come into the possession of the data controller. Includes any expressions of opinion and any indications of the intentions of the data controller, or any other person, in respect of the individual.

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

- Racial or ethnic origin
- Political opinion
- Religious or beliefs of a similar nature
- Trade union membership
- Physical or mental health or condition
- Sexual life
- Commission of alleged commission of any offence
- Criminal proceedings or convictions.

Data controller – Person who decides the purpose for which personal data is to be processed. In this instance **the Council** is the data controller for all personal data.

Data processor – A person (other than an employee of the data controller) who processes personal data on behalf of a data controller.

Data subject – An individual who is the subject of personal data.

Principles – There are eight data protection principles which personal data must be processed in accordance with. These are set out in Section 4.

Processing – means obtaining, recording or holding information or data or carrying out any operation or set of operations on the information or data, including any of the following:

- Organisation, adaptation or alteration
- Retrieval, consultation or use
- Disclosure or making available
- Destruction, erasure or alignment of the information or data.

4. The Principles of Data Protection

The Act contains **Eight Principles** relating to the collection, use, processing and disclosure of data. These Principles are legally enforceable and constitute good information handling practice.

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.

5. Handling of personal and/or sensitive information

Hertsmere Borough 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.
- 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.

The Act also grants rights to individuals. 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 the 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 trained to do so and 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, and performance with handling personal information are 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.
- Any Council forms requesting personal information will contain a fair collection notice giving details of the reasons for the collection and use of the information. Examples of such notices are available on the Council's intranet and in its guidance booklets for staff and Members.

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 departments 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 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 Hertsmere Borough Council. All contractors, consultants, partners or other servants or agents of Hertsmere Borough 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.

6. Responsibilities

The overall responsibility for the efficient administration of the Data Protection legislation lies with **the Council** and is exercised through the Chief Executive.

Day to day responsibility for administration and compliance with the Act is undertaken by the Directors and their staff, in relation to compliance with the Act's provisions within their respective areas of authority and responsibility. In some cases this may involve joint responsibilities and all staff should cooperate with their colleagues and act in compliance with and in the spirit of the Act.

All officers and Members have a duty to observe the principles of the Act and the procedures referred to in this document.

Members:
Members may be regarded as data controllers if they process personal data either manually or by computer, whether on their own equipment of on equipment provided to them by the Council.

Where holding and processing personal data about individuals in the course of undertaking Council business, a Member will be covered by the authority's notification and has the same responsibilities in respect of data protection as an employee of the Council.

When acting on behalf of a political party they will be covered by their own party's notification, but if they are acting on behalf of a resident Members will need to notify the Information Commissioner individually.

All individuals have a responsibility to ensure that any personal data is treated confidentially. Personal data and information may be extracted from data which the Council holds. Care needs to be taken in handling personal data at any time. For example, unauthorised disclosure of data may occur by passing information in a telephone conversation, which is contained in a computer print-out or event inadvertently by someone reading a computer screen.

All individuals should ensure insofar as practicable, personal data is treated in an appropriate manner which respects its confidential nature. Personal data should be retained securely. Personal data should not be left unattended on a desk or in a room or be visible on a computer screen to an unauthorised person.

The Council expects all of its Members and officers to comply fully with this policy and the principles of the Data Protection legislation. Disciplinary action may be taken against any employee who breaches any of the instructions or procedures in this policy. A disclosure of information by a Member in breach of the Data Protection provisions is a breach of the Code of Conduct. Any Council employee that is found guilty of a criminal offence under the Act may face disciplinary action from the Council.

Any Council employee, contractor, or councillor who is accused of a criminal offence under the Act must report it immediately to the Information Officer. Equally, any Council employee, contractor or councillor who suspects a criminal offence has been committed must report it to the Information Officer.

7. Implementation

Hertsmere Borough council has appointed an Information Officer. Designated Information Administrators have also been identified in all departments. 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 cascade data protection training, for staff within the council;
- the development of best practice guidelines;
- carrying out compliance checks to ensure adherence, throughout the authority, with the Data Protection Act.

Training sessions will be run on a quarterly basis in conjunction with Freedom of Information training. Refresher courses will also be provided on a regular basis.

Where possible, the Council will make use of a variety of training methodologies including e-learning, to support and promote the training of staff and members in Data Protection.

8. Disclosures

The Council reserves the right to disclose information under certain circumstances where allowed by law.

Disclosures routinely made by the Council are listed in the Council's notification with the Information Commissioner.

When a request for disclosure is made the Council will consider each request individually and where a disclosure takes place, the Council will only disclose the minimum amount required.

In order to improve service delivery and to meet its responsibilities, the Council may enter into data sharing agreements with other organisations. Where this is the case, the Council will ensure that an Information Sharing Protocol is in place which ensures the data sharing is in compliance with the law and this policy.

9. Notification to the Information Commissioner

The Information Commissioner maintains a public register of data controllers. The 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 Information Administrators will be responsible for notifying and updating the Information Officer of the processing of personal data, within their department.

The Information Officer will review the Data Protection notification document with designated Information Administrators annually, prior to notification to the Information Commissioner.

Any changes to the notification document 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.

10. Contact Details

Hertsmere Borough Council
Information Officer
Hertsmere Borough Council
Civic Offices
Elstree Way
Borehamwood
WD6 1WA

Phone: 020 8207 2277
Email: foi@hertsmere.gov.uk

Information Commissioner
Further information and explanation of the Data Protection Act can be found on www.ico.gov.uk or by writing to the Information Commissioner at the following address:
The Information Commissioner's Office
Wycliff house
Water Lane
Wilmslow
SK9 5AF

Improvement and Development Agency
Further guidance on Data Protection for Members has been published by the Improvement and Development Agency (IDeA) and can be accessed via their website www.idea.gov.uk.

October 2007