Breckland District Council

Data Protection Act Policy

July 2014

Democratic Services

Document Control and History

Version Control			
Issue No.	Author	Issue Date	Reasons for Issue
1	Susan Allen	July 2014	To up-date the current Policy

Approval of draft and final approval process			
Issue No.	Approval Process	Name	Signature and Date

CONTENTS

Introduction

Breckland District Council is committed to protecting the rights and privacy of all people with regard to the processing of personal data. During the course of our activities we will collect, store and process personal information about our staff, customers, suppliers and other third parties. We recognise the need to treat it in an appropriate and lawful manner and all processing will be conducted in accordance with the Data Protection Act 1998 and any subsequent amendments and everyone's rights with regard to how their personal information is handled.

The Policy applies to all employees and members of Breckland District Council. Any breach of the Data Protection Act 1998 and any subsequent amendments of the Council's Data Protection Policy will be taken seriously and may be considered to be a breach of the Members' Code of Conduct or the staff disciplinary procedures. As a matter of good practice, other agencies and individuals working with the Council, who have access to personal information, will be expected to read and comply with this Policy.

This Policy is open to all internal and external stakeholders and is available to view on the Council's website: www.breckland.gov.uk

Scope – Policy Aim

The types of information that we may be required to handle include details of current, past and prospective employees, suppliers, residents and others that we communicate with. The information, which may be held on paper or on a computer or other media, is subject to certain legal safeguards specified in the Data Protection Act 1998 and any subsequent amendments (the Act) and other regulations. The Act imposes restrictions on how we may use that information.

This Policy has been approved by Breckland District Council. It sets out the rules on data protection and the legal conditions that must be satisfied in relation to the obtaining, handling, processing, storage, transportation and destruction of personal information.

This Policy does not form part of any employee's contract of employment and may be amended at any time.

If you consider that the Policy has not been followed in respect of personal data about yourself or others you should raise the matter with your line manager or the Monitoring Officer. The Monitoring Officer is: Vicky Thomson, Assistant Director – Democratic Services, e-mail: vicky.thomson@breckland-sholland.gov.uk.

Any questions or concerns about the operation of this Policy should be referred to the Monitoring Officer or the Legal Services Coordinator.

Legislation or Executive Summary

The Data Protection Act 1998 and any subsequent amendments (referred to elsewhere in this policy as 'the Act') regulates the way in which personal information about individuals is obtained stored, used and disclosed. Individuals have the right to see the data stored about them, to require modifications of the data if it is wrong and in certain cases, to compensation. It applies to data held on computer or in a manual filing system. The Act provides conditions for the processing of any personal data and makes a distinction between personal data and 'sensitive' personal data (see Glossary of Terms).

Policy Consultation and Consideration

Corporate Management Team; Portfolio Holder; and Cabinet.

Policy Statement

1.1 Definition of Data Protection Terms

Data is information which is stored electronically, on a computer, or in certain paper-based filing systems.

Data Subject for the purpose of this Policy includes all living individuals about whom we hold personal data. A data subject need not be a UK national or resident. All data subjects have legal rights in relation to their personal data.

Personal data means data relating to a living individual who can be identified from that data (or from that data and other information in our possession). Personal data can be factual (such as a name, address or date of birth) or it can be an opinion (such as a performance appraisal).

Data controllers are the people who or organisations which determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Act. Breckland Council is the data controller of all personal data used in our business.

Data users include employees whose work involves using personal data. Data users have a duty to protect the information they handle by following our data protection and security policies at all times.

Data processors include any person who processes personal data on behalf of a data controller. Employees of data controllers are excluded from this definition but it could include suppliers which handle personal data on our behalf.

Processing is any activity that involves use of the data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transferring personal data to third parties.

Sensitive personal data includes information about a person's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition or sexual life, or about the commission of, or proceedings for, any offence committed or alleged to have been committed by that person, the disposal of such proceedings or the sentence of any court in such proceedings. Sensitive personal data can only be processed under strict conditions, and will usually require the express consent of the person concerned.

1.2 Data Protection Principles

The aim of this policy is to ensure that Breckland District Council complies with the eight enforceable principles of good practice when processing personal data. These provide that personal data must be:

- Processed fairly and lawfully;
- Processed for limited purposes and in an appropriate way;
- Adequate, relevant and not excessive for the purpose;

- Accurate;
- Not kept longer than necessary for the purpose;
- Processed in line with data subjects' rights;
- Secure; and
- Not transferred to people or organisations situated in countries without adequate protection.

1.3 Fair and Lawful Processing

The Act is intended not to prevent the processing of personal data, but to ensure that it is done fairly and without adversely affecting the rights of the data subject. The data subject must be told who the data controller is (in this case Breckland District Council), who the data controller's representative is (in this case the Monitoring Officer), the purpose for which the data is to be processed, and the identities of anyone to whom the data may be disclosed or transferred.

For personal data to be processed lawfully, certain conditions have to be met. These may include, among other things, requirements that the data subject has consented to the processing, or that the processing is necessary for the legitimate interest of the data controller or the party to whom the data is disclosed. When sensitive personal data is being processed, more than one condition must be met. In most cases the data subject's explicit consent to the processing of such data will be required.

Data about staff may be processed for legal, personnel, administrative and management purposes and to enable the data controller to meet its legal obligations as an employer, for example to pay staff, monitor their performance and to confer benefits in connection with their employment.

Examples of when sensitive personal data of staff is likely to be processed are set out below:

- Information about an employee's physical or mental health or condition in order to monitor sick leave and take decisions as to the employee's fitness for work;
- The employee's racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation;
- In order to comply with legal requirements and obligations to third parties

1.4 Processing for limited purposes

Personal data will only be processed for the specific purposes notified to the data subject when the data was first collected or for any other purposes specifically permitted by the Act. This means that personal data will not be collected for one purpose and then used for another. If it becomes necessary to change the purpose for which the data is processed, the data subject will be informed of the new purpose before any processing occurs.

1.5 Adequate, Relevant and Non-Excessive Processing

Personal data will only be collected to the extent that it is required for the specific purpose notified to the data subject. Any data which is not necessary for that purpose will not be collected in the first place.

1.6 Accurate Data

Personal data will be accurate and kept up to date. Information which is incorrect or

misleading is not accurate and steps will therefore be taken to check the accuracy of any personal data at the point of collection and at regular intervals afterwards. Inaccurate or out-of-date data will be destroyed.

1.7 Data Retention

Personal data will not be kept longer than is necessary for the purpose. This means that data will be destroyed or erased from our systems when it is no longer required.

1.8 Processing in line with Data Subject's Rights

Data will be processed in line with data subjects' rights. Data subjects have a right to:

- Request access to any data held about them by a data controller;
- Prevent the processing of their data for direct-marketing purposes;
- Ask to have inaccurate data amended;
- Prevent processing that is likely to cause unwarranted substantial damage or distress to themselves or anyone else; and
- Object to any decision that significantly affects them being taken solely by a computer or other automated process.

1.9 Data Security

We will ensure that appropriate security measures are taken against unlawful or unauthorised processing of personal data, and against the accidental loss of, or damage to, personal data.

The Act requires us to put in place procedures and technologies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third-party data processor if he agrees to comply with those procedures and policies, or if he puts in place adequate measures himself.

Maintaining data security means guaranteeing the confidentiality, integrity and availability of the personal data, defined as follows:

- **Confidentiality** means that only people who are authorised to use the data can access it.
- **Integrity** means that personal data should be accurate and suitable for the purpose for which it is processed.
- **Availability** means that authorised users should be able to access the data if they need it for authorised purposes. Personal data should therefore be stored on our central computer system instead of individual PCs.

Security procedures include:

- **Entry controls**. Any stranger seen in entry-controlled areas should be reported.
- **Secure lockable desks and cupboards**. Desks and cupboards should be kept locked if they hold confidential information of any kind. (Personal information is always considered confidential.)
- **Methods of disposal**. Paper documents should be shredded. Floppy disks, memory sticks and CD-ROMs should be physically destroyed when they are no longer required.
- **Equipment**. Data users should ensure that individual monitors do not show

confidential information to passers-by and that they log off from their PC when it is left unattended.

2.0 Subject Access Requests

A formal request from a data subject for information that the Council holds about them must be made in writing. A £10.00 fee is payable by the data subject for provision of this information. Any member of staff who receives a written request should forward it to the Democratic Services Officer immediately.

2.1 Providing Information to Third Parties

Any member of staff dealing with enquiries from third parties should be careful about disclosing any personal information held by us. In particular they should:

- Check the identity of the person making the enquiry and whether they are legally entitled to receive the information they have requested.
- Suggest that the third party put their requirement in writing so the third party's identity and entitlement to the information may be verified.

3.0 Implementation

Responsibilities under the Data Protection Act

Overall responsibility for compliance with the Act lies with the Monitoring Officer in conjunction with the Legal Services Coordinator. The Monitoring Officer will:

- Assess the understanding of the obligations of Breckland Council under the Act;
- Be aware of the authority's current compliance status;
- Identify and monitor problem areas and risks, and recommend solutions;
- Promote clear and effective procedures and offer guidance to staff on data protection;
- Develop best practice guidelines; and
- Carry out compliance checks to ensure adherence with the Act throughout the authority.

Day to day responsibility for compliance with this Policy is delegated to the Council's Corporate Management Team (CMT). CMT will ensure that the Legal Services Coordinator is informed of all computer and manual systems within the respective service areas that contain personal data.

The administration, day-to-day matters and the registration of systems and Subject Access Requests is delegated to the Legal Services Coordinator in conjunction with the Democratic Services Officer.

All staff are responsible for ensuring that:

- All personal data they hold, whether electronically or manually, is kept secure; and
- Personal information is not disclosed deliberately or accidentally either electronically, orally or in writing to any unauthorised third party.

Members can be regarded as Data Controllers in their own right if they process personal data

either manually or by computer, whether on their own equipment or on equipment provided to them by the Council. In this case, members must notify the Information Commissioner of all purposes for which they hold and process personal data.

Where holding and processing personal data about individuals in the course of undertaking Council business, the member will be covered by Breckland District Council's Notification, and have the same responsibilities in respect of data protection as an employee of the authority.

4.0 Management Control and Organisation

Breckland District Council will provide suitable management and control arrangements for all elements covered by the Data Protection Act 1998. The Monitoring Officer, the Legal Services Coordinator and the Member Services Team will play a part in the Council's arrangements for dealing with aspects of the Act. The Council will seek legal advice if and when required.

5.0 Monitoring

This policy will be reviewed every two years to ensure it is achieving its stated objectives. A review may be required earlier if legislation changes require the Policy to be updated.

6.0 Related Policies and Strategies

Freedom of Information Policy and Data Subject Access Request Form

7.0 Appendices

None.