Appendix 1

DATA PROTECTION POLICY

DATA PROTECTION ACT 1998

Sara J Freckleton
Borough Solicitor
Tewkesbury Borough Council
Council Offices
Gloucester Road
Tewkesbury
GL20 5TT
Tel No. 01684 272011

Sara.freckleton@tewkesbury.gov.uk

Revised October 2013

DATA PROTECTION POLICY

Introduction

This Policy is intended to assist the Council to comply fully with the requirements set out in the Data Protection Act 1998. It is the aim of the Council that all staff are properly trained, fully informed of their obligations under the Act and are aware of their personal liabilities.

The advice and policy statements it contains are applicable to all Council staff and non-Council staff who have access to Council-owned personal data.

The Council may take disciplinary action in the case of any employee acting in breach of the Data Protection legislation and/ or this Policy.

This Policy document applies only to information covered by the Data Protection Act 1998 and will be updated/amended as necessary. A monitoring process will also be developed to ensure compliance with this Policy.

The Freedom of Information Act 2000 also gives rights of access to all types of recorded information (personal and non-personal information) held by the Council (subject to 23 exemptions). This Policy takes into account the requirements of the Freedom of Information Act 2000 as appropriate.

In preparing this Policy the provisions of the Human Rights Act 1998 have been taken into account.

Applicability

This Policy applies to every individual in the Council who has access to personal data about other individuals such as Council clients, customers, employees, Members and third parties, such as suppliers or contractors.

The Council's Responsibility – A Summary

There are a series of definitions that need to be understood in the context of the data protection. These definitions derive from the Data Protection Act 1998 and are set out in full in Appendix 1.

The following chart summarises the provisions of the Act. The Council has a duty to comply with the data protection principles in relation to all data that is defined as personal. The Act gives individuals various rights in respect of personal data held about them by the Council.

WHAT'S IT ALL ABOUT

We have a duty to comply with →

in relation to all →

DATA

ie. information that is (or is intended to be) processed

- automatically eg. questionnaires, computer records

or

- as part of a relevant filing system eg. index cards/cabinet.
-

that is ↓

PERSONAL

ie. relates to a living individual identifiable either from DATA or from DATA and any other information which the Council possesses.

THE DATA PROTECTION PRINCIPLES

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless consent is obtained, it is in the interest of the individual or in the public interest.

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 (we register "purposes" with the Registrar).

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, 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 the 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 certain protection is in place.

DATA PROTECTION POLICY

It is essential that the Council handles personal data that it holds on its customers, employees, Members and third parties responsibly and with integrity.

1.0 Responsibilities

1.1 All Council employees who have access to personal data in any form must comply with the requirements as set out in the Data Protection Act 1998.

Corporate Data Protection Policy – Employee Responsibilities

All Council employees are personally responsible and accountable for ensuring compliance with the provisions of the Data Protection Act 1998, in particular with the eight data protection principles. This applies to all personal data that is processed by the Council.

1.2 All managers are responsible for the application of this Policy within their areas of responsibility and must ensure that their staff and any other persons for whom they are responsible who have access to personal data are aware of and understand their responsibilities with regard to the Act.

Corporate Data Protection Policy – Manager Responsibilities

All managers are directly responsible for implementing this Policy within their areas of responsibility and for compliance with it by their staff.

2.0 Education and Training

2.1 It is intended that education and training on data protection issues will be provided on a regular basis, to all Council staff. It is a management responsibility to ensure that all staff receive sufficient data protection education and training to enable them to fulfil their data protection responsibilities.

Corporate Data Protection Policy – Education and training

All managers must ensure that all staff for whom they are responsible who process personal data receive education and training in data protection issues and have up to date knowledge in this area.

3.0 Off-Site Working

3.1 Personal data relating to Council customers, clients, employees, Members or third parties such as suppliers or contractors must not be removed from the Council offices by staff without the express authorisation of the appropriate manager. When Council-owned data is away from the Council offices, staff are solely responsible for the security of the data and must take reasonable precautions to prevent unauthorised persons gaining access to it.

Corporate Data Protection Policy – Off-site working

Council staff working off-site with Council-owned personal data must ensure that they abide by the provisions of the Data Protection Act 1998. In particular, Council-owned data which is taken off-site must be transferred and held securely, not transferred to a third party and must be used only for official Council business.

4.0 Notification

4.1 The Information Commissioner maintains a public register of data controllers. Each register entry includes the name and address of the data controller and a general description of the processing of personal data by a data controller. The Council has a number of register entries. Notification is the process by which a data controller's (the Council's) details are added to the register. The Data Protection Act 1998 requires that the Council notify all personal data. Failure to notify is a criminal offence.

Corporate Data Protection Policy – Notification

All managers must ensure that any additional purposes, other than those contained in their register entry, for which they are processing personal data are notified to the Data Protection Officer who can then amend the Council's register entries as appropriate.

5.0 Individuals' Rights

5.1 The Act gives rights to individuals (data subjects) in respect of personal data held about them by data controllers. These are mainly concerned with the:-

- right of information about the processing of personal data
- right of access to their personal data
- right to prevent processing likely to cause damage or distress
- right to prevent processing for the purposes of direct marketing
- right to prevent decision-making solely by automatic means
- right to seek compensation for damage or distress arising from any breach of the Act and, having established damage, to seek compensation for any associated distress
- right of rectification, blocking, erasure or destruction of personal data that are inaccurate or which contain an opinion which appears to be based on the inaccurate data
- right to request the Commissioner to assess whether or not it is likely that any processing of personal data by a data controller has been carried out in compliance with the Act

5.2 Depending on the circumstances, the penalties for any breach of the rights of data subjects may be as significant to individuals and organisations as the penalties for criminal offences.

Corporate Data Protection Policy – Individual Rights

The Council will, as far as practicable, ensure that all individuals whose details are held by the Council are aware of the way in which that information is held, used and disclosed.

6.0 Subject Access

6.1 An individual has the right to access a copy of their personal data held by a data controller. This is called the subject access right. A request for subject access has to be made in writing (which includes transmission by electronic means) and must be complied with within 40 days. The Data Protection Officer will issue guidance on how subject access requests are to be handled, to take account of local circumstances. Any officer who receives a subject access request must immediately contact the Data Protection Officer and provide details of the request.

Corporate Data Protection Policy – Handling of Subject Access Requests

Managers must be aware of the procedure for handling subject access requests within their department. All subject access requests shall be dealt with in the way that the Data Protection Officer prescribes.

7.0 Sensitive Personal Data

Sensitive data may be included in the personal data the Council processes, for instance data which reveals racial or ethnic origin, political opinions, religions, beliefs, trade union membership or concerning health or sex life. The Council will process such data in such a way as to ensure that privacy is maintained and will only be processed with the explicit consent of the Data Subject.

Corporate Data Protection Policy – Sensitive Data

The Council will ensure that adequate security measures are taken so that privacy is preserved whenever and wherever processing of sensitive data takes place and such processing will only take place with the explicit consent of the Data Subject.

8.0 Technical and Organisational Security

8.1 The Council has implemented appropriate security measures as required under the Data Protection Act 1998. In particular, unauthorised staff and other individuals are prevented from gaining access to personal information. Appropriate physical security is in place, with visitors being received and supervised at all times within the Council's building where information about individuals is stored. The general public visiting the Council's building should not feel that the measures are restrictive or oppressive, the measures are there to protect the Council's data.

8.2 Computer systems are installed with user profile-type password controls and, where necessary, audit and access trails to establish that each user is fully authorised. In addition, employees are fully informed about overall security procedures and the importance of their role within those procedures. Security arrangements are reviewed regularly. All reported breaches or potential weaknesses are investigated and, where necessary, further or alternative measures will be introduced to secure the data. Such reports are received by the Data Protection Officer for the Council, who will liaise with IT and/or building Security staff as necessary.

8.3 All staff are informed and frequently reminded about the limits of their authority on disclosing information both inside and outside the Council. Details will only be

disclosed on a need-to-know basis within the Council. Where details need to be passed outside the Council it will, in general, be done with the person's consent, except where this is not possible or where it is required by law, allowed under the Data Protection Act exemptions (such as crime prevention/detection, to prevent injury, etc), or where it is in the person's vital interest. Any unauthorised disclosure will be dealt with under the Council's disciplinary procedures.

Corporate Protection Policy – Technical and Organisational Security

The Council will take sufficient steps to secure the Council's data through IT and organisational measures.

9.0 Offences

9.1 The Act creates a number of offences. A data controller is liable to commit an offence under the Act if he or she:-

- fails to notify processing of personal data, where required
- fails to notify changes to processing of personal data
- fails to comply with an enforcement notice
- makes a statement in purported compliance with an information notice which he or she knows to be false or recklessly makes a statement which is false in a material respect
- unlawfully obtains personal data
- unlawfully sells personal data
- unlawfully offers personal data for sale
- unlawfully obtains personal data by requiring someone to exercise their subject access rights in connection with employment or the provision of services
- obstructs a person in the execution of a warrant
- fails without reasonable excuse to give any person executing such a warrant such assistance as he or she may reasonably require

9.2 Failure to comply with the requirements of the Act could result in Council employees being held liable under the Act for their actions. If an employee of the Council is found guilty of committing an offence they could be liable for a fine of up to £5,000 in the Magistrates' Court or an unlimited fine in the Crown Court.

Corporate Data Protection Policy – Offences

Any member of staff receiving notice of prosecution regarding offences under the Data Protection Act 1998 must immediately notify the Data Protection Officer

10.0 Further Information

10.1 If you require further information or guidance on data protection issues contact the Data Protection Officer, Sara J Freckleton, on extension 2010, or at Tewkesbury Borough Council, Council Offices, Gloucester Road, Tewkesbury, Gloucestershire, GL20 5TT.

CORPORATE DATA PROTECTION POLICY STATEMENTS

1. Employees Responsibilities

All Council employees are personally responsible and accountable for ensuring compliance with the provisions of the Data Protection Act 1998, in particular with the eight data protection principles. This applies to all personal data that is processed by the Council.

2. Managers Responsibilities

All managers are directly responsible for implementing this Policy within their areas of responsibility and for compliance with it by their staff.

3. Education and Training

All managers must ensure that all staff for whom they are responsible who process personal data receive education and training in data protection issues and have up to date knowledge in this area.

4. Off-site Working

Council staff working off-site with Council-owned personal data must ensure that they abide by the provisions of the Data Protection Act 1998. In particular, Council-owned data which is taken off-site must be transferred and held securely, not transferred to a third party and must be used only for official Council business.

5. Notification

All managers must ensure that any additional purposes, other than those contained in their register entry, for which they are processing personal data are notified to the Data Protection Officer who can then amend the Council's register entries as appropriate.

6. Individual Rights

The Council will, as far as practicable, ensure that all individuals whose details are held by the Council are aware of the way in which that information is held, used and disclosed.

7. Handling of Subject Access Requests

Managers must be aware of the procedure for handling subject access requests within their department. All subject access requests shall be dealt with in the way that the Data Protection Officer prescribes.

8. Sensitive Data

The Council will ensure that adequate security measures are taken so that privacy is preserved whenever and wherever processing of sensitive data takes place and such processing will only take place with the explicit consent of the Data Subject.

9. Technical and Organisational Security

The Council will take sufficient steps to secure the Council's data through IT and organisational measures.

10. Offences

Any member of staff receiving notice of prosecution regarding offences under the Data Protection Act 1998 must immediately notify the Data Protection Officer

APPENDIX 1

Data

Data means information which:-

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose
(b) is recorded with the intention that it should be processed by means of such equipment
(c) is recorded as part (or with the intention that it should form part) of a relevant filing system (i.e. any set of information relating to individuals relating to information to the extent that, although not processed as in (a) above, the set is structured by reference to individuals or by reference to criteria relating to individuals, in, or
(d) does not fall within paragraph (a), (b) or (c) but forms part of an accessible health record as defined by Section 68 and which can be summarised here as a health record, educational record (local education authority schools and special schools only).

Personal Data

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

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

Data Controller

Data controller means a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed. (The Council in this policy is the Data Controller.)

Data Subject

Data subject means an individual who is the subject of personal data.

Processing

Processing, in relation to information or data, means obtaining, recording or holding the information or data (which includes, in relation to personal data, obtaining or recording the information to be contained in the data) or carrying out any operation or set of operations on the information or data, including:-

- organisation, adaptation or alteration of the information or data
- retrieval, consultation or use of the information or data (which, in relation to personal data, includes disclosing the information contained in the data) by transmission, dissemination or otherwise making available, or
- alignment, combination, blocking, erasure or destruction of the information or data

Relevant Filing System

The relevant filing system means any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

Sensitive Personal Data

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.