Epping Forest District Council

Corporate Policy

Data Protection Policy

1. INTRODUCTION

1.1 Epping Forest District Council ('the Council') is a data controller pursuant to the Data Protection Act 1998 ('the Act'). The Council is fully committed to compliance with the requirements of the Act, which came into force on 1 March 2000.

1.2 The Council will establish and follow procedures that aim to ensure that all employees, elected members, contractors, agents, consultants, partners or other servants of the authority (for the purposes of this policy these are collectively known as data 'users'), who have access to personal data held by or on behalf of the authority, are fully aware of and abide by the Council's duties and responsibilities under the Act.

1.3 The Information Commissioner maintains a public register of data controllers and the Council is registered as such. The Act 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 Council also requires all of its elected members to individually register as a data controller with the Information Commissioner.

2. POLICY STATEMENT

2.1 In order to carry out its functions, 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, customers and suppliers. In addition, the Council may be required by law to collect and use information in order to comply with requirements of central government. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it is held on paper, in computer records or recorded by any other means. There are safeguards in the Data Protection Act to ensure this.

2.2 The Council regards the lawful and correct treatment of personal information as very important to the successful and efficient performance of its operations and functions, and to maintaining confidence between the authority and those with whom it deals. To this end, the Council fully endorses and adheres to the principles of data protection as set out in the Act. All officers and members must comply with this policy, and be familiar with the confidentiality issues involved.

3. POLICY BACKGROUND

3.1 The purpose of this policy is to ensure that the Council's officers and members are clear about the purpose and principles of data protection, and that the authority has guidelines and procedures in place that are followed consistently.

3.2 The Act regulates the 'processing' of personal data relating to living and identifiable individuals (known as 'data subjects'). Personal data is information relating to a living individual, who can be identified from:

- that data; or
- that data and other information which is in the possession of, or is likely to come into the possession of the data controller (i.e. the Council).

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

3.4 The act of processing personal data includes the obtaining, holding, using or disclosing of such information, and covers computerised records as well as manual filing systems and card indexes. The Act stipulates that anyone processing (i.e. using) personal data must comply with eight principles of good practice. These principles are legally enforceable, and require that personal information:

- be processed fairly and lawfully and in particular, not be processed unless specific conditions are met;
- be obtained only for one or more specified and lawful purposes and not be further processed in any manner incompatible with that purpose or those purposes;
- be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed;
- be accurate and where necessary, kept up to date;
- not be kept for longer than is necessary for that purpose or those purposes;
- be processed in accordance with the rights of data subjects under the Act;
- be kept secure i.e. protected by an appropriate degree of security; and
- 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.

3.5 The Act provides conditions for the processing of any personal data. It also makes a distinction between personal data and 'sensitive' personal data. Sensitive personal data is data consisting of information relating to an individual's:

- racial or ethnic origin;
- political opinions;
- religious beliefs or beliefs of a similar nature;
- trade union membership;
- physical or mental health or condition (this could include disability);
- sexual life;
- commission or alleged commission of an offence and proceedings for any offence committed or alleged, including sentencing.

3.6 The 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 only to the extent that it is needed to fulfil operational needs or to comply with 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, including the right to be informed that processing is being undertaken, the right of access to personal information, the right to prevent processing in certain circumstances, and the right to correct, rectify, block or erase information regarded as wrong information.

3.7 In addition, the Council will ensure that:

- it designates an officer with specific responsibility for data protection across the authority (the 'Data Protection Officer');
- 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 the handling of 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;

- all systematic data sharing is carried out under a written agreement setting out the scope and limits of the sharing, and that any disclosure of personal data is in compliance with approved procedures.

3.8 The Council requires all of its elected members to comply with this policy. The authority also requires that each member be registered as an individual data controller in connection with personal data that they process as part of their community casework activities, and to be aware of their duties and responsibilities under the Act. The Data Protection Officer handles the annual registration of members as data controllers with the Information Commissioner.

3.9 All of the Council's officers will take appropriate 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 hard-copy records or documents containing personal and 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; and
- passwords are such that they are not easily compromised.

3.10 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.

3.11 All contractors that use personal data supplied by the Council will be required to confirm that they will abide by the requirements of the Act with regard to that information.

4. SUBJECT ACCESS

4.1 The subject access provisions of the Act promote the principles of transparency and accountability. Subject access enables individuals to understand how their personal data is being used by the Council, to check the accuracy of information that the authority holds, and to exercise rights over the processing of such data. Any individual, who is subject to the processing of personal data, has a right of access to the personal information that the Council holds about them.

4.2 The designated Data Protection Officer will consider and respond to all Subject Access Requests. All officers should be able to recognise a Subject Access Request and must ensure that requests are passed to the Data Protection Officer immediately. The Council has adopted a Subject Access Request Protocol setting out how it handles requests for personal data, which is available is on the Corporate Policies section of the Council's intranet.

5. DATA SHARING

5.1 The Council is often requested to disclose or 'share' personal data in connection with the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of tax. Whilst it is likely to be in the public interest for the Council to assist investigations in this respect, the authority is committed to ensuring that all disclosures of personal data are fair, and comply fully with the provisions of the Act.

5.2 The Council has adopted a Data Sharing Protocol setting out how it handles this type of request for personal data. The protocol applies only to data sharing requests made in relation to crime and taxation related maters, and does not affect the operation of information sharing agreements in place between the Council and relevant organisations. The protocol similarly does not apply in circumstances where the Council is legally obliged to share particular personal data with a named organisation, or is expressly permitted to disclose information for certain purposes. The protocol is available is on the Corporate Policies section of the intranet.

5.3 All agreements or formal arrangements for the sharing of personal data with other organisations must be approved by the Corporate Governance Group and be signed by the Chief Executive on behalf of the Council.

6. WHY USERS & MANAGERS MUST FOLLOW THIS POLICY

6.1 A breach of this policy by a member of staff is likely to lead to disciplinary action being taken. Investigation of any breach of the policy will also include a review of relevant data management procedures.

6.2 A breach of the policy by an elected member is a potential breach of the Council's Code of Member Conduct.

6.3 If an individual's personal information is disclosed outside its intended purpose, they have a right to sue the person responsible. Individual officers and members of the Council may be prosecuted under the Act, not just the authority as a whole.

6.4 The Computer Misuse Act 1990 identifies the legal framework for the definition of and prosecution for unauthorised use or misuse of computers and computer systems. Whilst this Act is particularly intended to deal with unauthorised accesses from outside the organisation ('hackers'), it deals equally with unauthorised accesses from inside. Penalties under the Act fall into two main categories:

(a) Unauthorised access - Anyone gaining access, or attempting to gain access to computer data they are not authorised to see, may face a fine of up to £2,000 or six months in prison, or both; and

(b) Ulterior intent or unauthorised modification - Anyone accessing data with an ulterior motive, or modifying data without authorisation, may be sentenced to up to five years in prison or an unlimited fine, or both.

6.5 Security breaches involving personal data can cause harm and distress to the individuals that they affect. Whilst not all security breaches have such consequences, they can still cause serious embarrassment or inconvenience to the people concerned.

6.6 The Council has adopted a Personal Data Breach Management Protocol setting out how it handles the loss or unauthorised disclosure of personal data, which must be followed in respect of all security breaches that involve personal data. The procedures set out in the protocol, which is available on the Corporate Policies section of the intranet.

7. DATA SECURITY

7.1 The Council will comply with the seventh principle of the Data Protection Act and implement appropriate technical and organisational measures to guard against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

7.2 It is essential that users, understand the extent of their authority to use and access systems. Computers used for more than one purpose and those connected to the Council's corporate network provide the potential for access to a large number of systems and to a great deal of personal, private and confidential data.

7.3 This policy makes it the responsibility of all users to guard and protect their ability to access systems that they have authority to use. Passwords must not be written down or passed on (even to line managers or ICT) and computers must not be left logged in when unattended, unless password protected or locked.

7.4 Any user finding that they have access to systems and data which they are not authorised to use must report this to their supervisor or manager, the Data Protection Officer, and to the ICT Unit, in order that the access may be removed. Any employee with authority to access data that is no longer necessary to their work must ask for the access to be removed.

7.5 Any employee who knows that unauthorised access is taking place must report this to their supervisor or manager, the Data Protection Officer, and to ICT, in order that access may be removed.

7.6 If it is necessary to send personal data externally (i.e outside the Council's internal network), one of the following options must be used in the following order of preference:

(a) secure email via the GCSX facility to other secure government recipient addresses (e.g., PNN, GSI, other GCSX etc.).
(b) secure email via the Council's corporate encryption system to non-secure government recipients (e.g. DVLA);
(c) secure email via the corporate encryption system to other recipients, with the prior approval of the Data Protection Officer; or
(d) encrypted CD sent via secure means (e.g. registered post).

7.7 CDs that contain personal data must always be encrypted. The Council does not permit the use of USB memory sticks for the transfer of personal data, in any circumstances. Information about the corporate encryption system, the encryption of CDs and other secure electronic data transfer methods, can be obtained from ICT.

7.8 Line manager authorisation is required for use of the GCSX secure email facility. Guidance on the use of GCSX can be found on ITrain, the Council's e-Learning system for officers and members.

7.9 For personal data sent through the 'normal' postal system to a named individual, regard should always be had to the value, importance or sensitivity of the personal information and the impact of any loss of such information for an individual to whom it relates. Appropriate postal services (e.g. special delivery, recorded delivery etc.) should be considered as necessary when sending personal data by post.

7.10 Where an individual chooses to send personal information to the Council (e.g. their name and address), that information can be used in order to respond to the specific communication or enquiry.

7.11 The Council's ICT Security Policy covers the use of ICT equipment and systems and defines standards for appropriate security. This and other related ICT policies are available on the Corporate Policies section of the intranet.

8. USER ROLES & RESPONSIBILITIES

8.1 All officers are required to confirm their understanding of and agreement to this Data Protection Policy, and to confirm that they have been made aware of their confidentiality and

data protection responsibilities. This will be achieved through the MetaCompliance policy management system.

8.2 All users are required to read, understand and accept any other policies and procedures that relate to any personal data that they may handle in the course of their work.

8.3 The Data Protection Policy will be issued to members at the commencement of each municipal year.

9. DIRECTORATE MANAGEMENT ROLES & RESPONSIBILITIES

9.1 All Directors (or other nominated officers) are responsible for the implementation of this Data Protection Policy within their individual service area(s), and for service compliance with the policy and the supporting data protection guidance.

9.2 Each of the Council's directorates or service areas where personal data is handled is responsible for drawing up its own operational procedures (including induction and training arrangements) to ensure that good data protection practice is established and followed. Owing to the wide variety and different levels of personal data collected and different uses made of information across the Council, it is not possible to issue a single corporate procedure to cover all directorates and service areas.

9.3 All directorate or service area level procedures must be in conformity with this Data Protection Policy and supporting data protection guidance. The Data Protection Officer can advise on the suitability of directorate or service area level policies and procedures.

10. CORPORATE ROLES & RESPONSIBILITIES

10.1 The designated Data Protection Officer leads corporate implementation and monitoring of compliance with this Data Protection Policy.

10.2 The Data Protection Officer also has overall responsibility for the provision of data protection training for the Council's officers and members. For officers, this will primarily be achieved through the use of a mandatory electronic learning module. Training will be provided to members on an annual basis, as part of the authority's Member Development Programme.

10.3 The Data Protection Officer also has the following responsibilities:

(a) to provide advice and guidance on the provisions and requirements of the Act and this Data Protection Policy;
(b) to ensure that the Council's corporate registration as a data controller, and those of individual members, is accurately maintained at all times;
(c) to manage requests for access to personal data and the exercise of other rights under the Act,, including subject access and data sharing requests;
(d) to provide advice and guidance in respect of unusual or controversial disclosures of personal data, and contracts with data processors;
(e) to investigate incidents and complaints in relation to the security or disclosure of personal data held by the Council; and
(f) to report to the Corporate Governance Group on relevant data protection matters.

10.4 The Corporate Governance Group is responsible for monitoring and reviewing the Council's corporate governance framework, including data protection matters.

11. FURTHER INFORMATION

11.1 Additional information regarding this Data Protection Policy and guidance in respect of specific data protection matters can be obtained from the Council's designated Data Protection Officer. The Data Protection Officer can be contacted as follows:

Data Protection Officer,
Epping Forest District Council,
Democratic Services,
Civic Offices,
High Street,
Epping,
Essex, CM16 4BZ.

☎ (01992) 564180
✉ dataprotection@eppingforestdc.gov.uk

11.2 A companion 'Guide to Data Protection' is available on the Corporate Policies section of the intranet. The guide explains the eight principles of the Data Protection Act 1998 and procedures for dealing with personal data.

12. DOCUMENT HISTORY

12.1 The designated Data Protection Officer, in conjunction with the Assistant Director of Resources (ICT and Facilities Management) as appropriate, is responsible for the maintenance of this policy. The policy is subject to regular review to reflect, for example, relevant legislative changes, new case law, or revised guidance published by the ICO.

Prepared/Revised	Written by	Agreed/Authorised	Details of Change(s)
1 October 2010	ICT	Management Board	Baseline policy release
7 January 2011	ICT	Management Board	Released policy document
November 2012 (Annual Review)	S. Tautz (Data Protection Officer)	Management Board (28/11/12)	Revision to reflect: • additional options for sending personal information externally; • changes to corporate data protection responsibility; General update of policy text.
January 2013	N/A	N/A	Revised policy document issued (Metacompliance)
November 2013 (Annual Review)	S. Tautz (Data Protection Officer)	Corporate Governance Group (20/11/13)	Revision to reflect: • agreed responsibilities of Data Protection Officer; • protocols supporting the Data Protection Policy; • general update of policy text.
January 2014	N/A	N/A	Revised policy document published to intranet and website

April 2014	S. Tautz (Data Protection Officer)	S. Tautz (Data Protection Officer)	Policy updated as required to reflect new senior management structure. Republished to intranet and website.
November 2015 (Review)	S. Tautz (Data Protection Officer)	Corporate Governance Group (2/12/15)	Inclusion of requirements for member registration and approval of data sharing agreements. General update of policy text.
September 2017	S. Tautz (Data Protection Officer)	S. Tautz (Data Protection Officer)	Revision of contact details for Data Protection Officer.