Epping Forest District Council
www.eppingforestdc.gov.uk

Corporate Policy: Data Protection

1. INTRODUCTION

1.1 Epping Forest District Council ('the Council') is a data controller pursuant to the General Data Protection Regulation ('GDPR'). The Council is fully committed to compliance with the requirements of the GDPR, which came into force on 25 May 2018.

1.2 The Council has established procedures 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 GDPR and this Policy. The policy is intended to protect the Council from data security risks, including breaches of confidentiality and consequent reputational damage. Everyone who works for or with the Council has some responsibility for ensuring that personal data is collected, stored and handled appropriately.

1.3 The Data Protection Policy applies to all officers and elected members of the Council. A breach of the policy by a member of staff may lead to disciplinary action being taken. Inappropriate handing of personal data by an elected member may be a potential breach of the Council's Code of Member Conduct.

2. POLICY STATEMENT

2.1 The Data Protection Policy sets out the Council's commitment to the protection of personal data and how it implements that commitment with regards to the collection and use of personal data. The policy helps to ensure that the Council's officers and members are clear about the purpose and principles of data protection and that the authority has applies appropriate and consistent procedures to the processing of personal data.

2.2 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 GDPR to ensure this.

2.3 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 GDPR. All officers and members must comply with this policy, and be familiar with its requirements.

2.4 The Council will, through the use of appropriate management and system controls, monitoring and review:

(a) use personal data in the most efficient and effective way to deliver better services;
(b) strive to collect and process only the data or information which is needed;
(c) use personal data for such purposes as are described at the point of collection, or for purposes which are legally permitted;
(d) strive to ensure information is accurate;
(e) not keep information for longer than is necessary;
(f) securely destroy data which is no longer needed;
(g) take appropriate technical and organisational security measures to safeguard information (including unauthorised or unlawful processing and accidental loss or damage of data);
(h) ensure that information is not transferred abroad without suitable safeguards;
(i) ensure that there is general information made available to the public about their rights to access information; and
(j) ensure that the rights of people about whom information is held can be fully exercised under the GDPR.

3. PERSONAL DATA

3.1 The GDPR regulates the 'processing' of personal data relating to living and identifiable individuals (known as 'data subjects'). Personal data is any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.

3.2 This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organisations collect information about people. The GDPR applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria. This could include chronologically ordered sets of manual records containing personal data.

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. Personal data that has been pseudonymised (e.g. key-coded) can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

4. SPECIAL CATEGORIES OF PERSONAL DATA

4.1 The GDPR makes a distinction between personal data and 'special categories' of personal data. Special category personal data includes the following information about an individual, that is generally regarded to be 'sensitive' in nature:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

4.2 Special category data is more sensitive than regular personal data and requires a higher level of protection, these types of data could create more significant risks to a person's fundamental rights and freedoms, by putting them at risk of unlawful discrimination.

4.3 Personal data relating to criminal convictions and offences are not regarded as special categories of personal data, but similar extra safeguards apply to the processing of this type of data

5. DATA PROTECTION PRINCIPLES

5.1 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 GDPR stipulates that anyone processing (i.e. using) personal data must comply with a number of principles of good practice. These principles are legally enforceable, and require that personal information only be:

(a) processed lawfully, fairly and in a transparent manner in relation to individuals;

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

5.2 These principles are the minimum standards the Council strives to meet with respect to its handling of personal data.

6. USER ROLES & RESPONSIBILITIES

6.1 All officers of the Council are required to confirm their understanding of this Data Protection Policy and their agreement to comply with its provisions. This will be achieved through the Metacompliance policy management system.

6.2 All officers will, through appropriate training and responsible management, observe all forms of guidance, policies and procedures about the collection and use of personal data by the Council. All officers are required to understand and accept any other policies and procedures that relate to personal data that they may handle in the course of their work.

6.3 The Data Protection Policy will be issued to members at the commencement of their relevant term of office

7. CORPORATE ROLES & RESPONSIBILITIES

7.1 All Service Directors are responsible for the implementation of the Data Protection Policy within their individual service areas and for service compliance with the policy and the supporting data protection guidance.

7.2 Each service area in which personal data is processed, is responsible for developing and implementing appropriate operational procedures (including induction and training arrangements) to ensure that good data protection practice is established and followed in the handling and use of personal data.

7.3 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.

7.4 The Acting Chief Executive is the Council's Senior Information Risk Owner and is responsible and accountable for corporate information risk across the authority. The Corporate Governance Group is responsible for monitoring and reviewing the Council's corporate governance framework, including data protection compliance.

8. DATA PROTECTION OFFICER

8.1 The Council is required to designate an officer with specific responsibility for data protection across the authority (the 'Data Protection Officer'). The GDPR defines the main tasks of the Data Protection Officer, which are to:

(a) inform and advise the Council and its officers about obligations to comply with the GDPR and other data protection laws;
(b) monitor compliance with the GDPR and other data protection laws, and with the Council's data protection polices, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits;
(c) advise on, and monitor, data protection impact assessments;
(d) cooperate with the Information Commissioner; and
(e) be the first point of contact for the Information Commissioner and for individuals whose data is processed (employees, customers etc).

8.2 The Data Protection Officer leads corporate implementation and monitoring of compliance with this Data Protection Policy and also has the following additional responsibilities:

(a) managing requests for the application of data subject rights, including access to personal data;
(b) providing advice and guidance in respect of unusual or controversial disclosures of personal data and contracts with data processors;
(c) investigating incidents and complaints in relation to the security or disclosure of personal data held by the Council; and
(d) reporting to the Corporate Governance Group on relevant data protection matters.

9. PROCESSING PERSONAL DATA

9.1 The processing of personal data includes operation performed on the data (whether such operations are automated or not), including (but not limited to) collecting, recording, organising, structuring, storing, modifying, consulting, using, publishing, combining, erasing, and destroying the data.

9.2 The Council will, through the use of appropriate management policies 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 GDPR.

9.3 In addition, the Council will ensure that:

- all officers that manage and handle personal information understand that they are contractually responsible for following good data protection practice;
- all officers that manage and handle personal information are appropriately trained to do so;
- all officers that manage and handle personal information are 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.

9.4 The Council requires all of its elected members to comply with this policy. The authority also requires that each member be aware of their duties and responsibilities under the GDPR. The Data Protection Officer acts in a similar capacity for members of the Council and provides appropriate training.

9.5 All officers of the Council must take appropriate steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure and, in particular, 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.

9.6 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 GDPR. A breach of any provision of the GDPR 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 prosecutions, claims, proceedings, actions or payments of compensation or damages, without limitation.

9.7 All contractors that process personal data supplied by the Council are required to confirm that they abide by the requirements of the GDPR with regard to that information.

10. RIGHTS OF DATA SUBJECTS

10.1 The GDPR provides various rights for individuals. All officers must be able to recognise requests for the application of these rights and must ensure that requests are passed to the Data Protection Officer immediately.

10.2 The Council has adopted a Subject Rights Handling Protocol setting out how it handles requests for the application of these rights, which is available on the intranet.

(a) The right to be informed

The right to be informed encompasses the Council's obligation to provide 'fair processing information and emphasises the need for transparency over how such personal data is used. The information supplied about the processing of personal data will typically be provided through a privacy notice and must be:

- concise, transparent, intelligible and easily accessible;
- written in clear and plain language, particularly if addressed to a child; and
- free of charge.

(b) The right of access

Individuals have the right to access their personal data and supplementary information. The right of access allows individuals to be aware of and verify the lawfulness of the processing their personal data. Under the GDPR, individuals have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information, which will largely correspond to the information that provided privacy notices.

The subject access provisions of the GDPR 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.

The Data Protection Officer will consider and respond to all requests for access to personal data.

(c) The right to rectification

The GDPR gives individuals the right to have personal data rectified if it is inaccurate or incomplete. If the Council has disclosed personal data to a third-party organisation, it must contact such recipient and inform them of such rectification, unless this proves impossible or involves disproportionate effort. If asked to, the Council must also inform the individuals about such recipients.

The Data Protection Officer will consider and respond to all requests the rectification of personal data.

(d) The right to erasure

The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing. The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed;
- when the individual withdraws consent; when the individual objects to the processing and there is no overriding legitimate interest for continuing the processing;
- where the personal data was unlawfully processed (i.e. otherwise in breach of the GDPR);
- where the personal data has to be erased in order to comply with a legal obligation; and
- where the personal data is processed in relation to the offer of information society services to a child.

10.10 Under the GDPR, this right is not limited to processing that causes unwarranted and substantial damage or distress. However, if the processing does cause damage or distress, this is likely to make the case for erasure stronger. There are some specific circumstances where the right to erasure does not apply and the Council can refuse to deal with a request.

10.11 The Data Protection Officer will consider and respond to all requests for the erasure of personal data.

(e) The right to restrict processing

10.12 Individuals have a right to 'block' or suppress the processing of personal data. When processing is restricted, the Council is permitted to store the personal data, but not further process it and can retain just enough information about the individual to ensure that the restriction is respected in future. The Council is required to restrict the processing of personal data in the following circumstances:

- where an individual contests the accuracy of the personal data, until the accuracy of the personal data has been verified;
- where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and the Council is considering whether its legitimate grounds override those of the individual;
- when processing is unlawful and the individual opposes erasure and requests restriction instead; and
- if the personal data is no longer needed, but the individual requires the data to establish, exercise or defend a legal claim.

10.13 The Data Protection Officer will consider and respond to all requests for the restriction of the processing of personal data.

(f) The right to data portability

10.14 The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability. The right to data portability enables people to take advantage of applications and services that can use this data.

10.15 The Data Protection Officer will consider and respond to all requests for the application of the right to data portability.

(g) The right to object

10.16 Individuals have the right to object to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics

10.17 The Council must stop processing personal data used in the performance of a public task unless it can demonstrate compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or the processing is for the establishment, exercise or defence of legal claims.

10.18 The Data Protection Officer will consider and respond to all requests for the application of the right to object to the processing of personal data.

(h) Rights in relation to automated decision making and profiling

10.19 The GDPR contains protections for individuals in relation to automated individual decision-making (making a decision solely by automated means without any human involvement) and profiling (automated processing of personal data to evaluate certain things about an individual).

11. DATA SHARING

11.1 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 GDPR.

11.2 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 matters, and does not affect the operation of contracts with third-party organisation that involve the processing of personal data, or 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 intranet.

11.3 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 Acting Chief Executive on behalf of the Council.

12. DATA SECURITY

12.1 The Council will comply with the data security principle of the GDPR and implement protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

12.2 It is essential that all officers 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.

12.3 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.

12.4 Any officer that discovers that they have access to systems and data which they are not authorised to use, must report this to their line manager and ICT as soon as possible, in order that the access may be removed. Any employee with authority to access data that is no longer necessary to their work must seek the removal of such access without delay. Any officer that knows or suspects that unauthorised access to personal data is taking place, must report this to their line manager immediately.

12.5 Personal data should not be shared informally. In particular, it should never be sent through the corporate electronic mail facility (Microsoft Outlook), as this form of communication is not secure. If it is necessary to send personal data externally (i.e. outside the Council's internal network) by electronic means, advice in regard to options for the secure transfer of the data must be sought from the Assistant Director (ICT and Facilities Management.

12.6 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.

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

12.8 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 intranet.

13. DATA SECURITY BREACHES

13.1 The GDPR introduces more stringent duties on the Council to report personal data breaches to the Information Commissioner. The Council holds large amounts of personal data and takes every care to protect this information and to avoid a data security breach. However, in the unlikely event of data being lost or disclosed inappropriately, it is vital that swift action is taken to minimise any associated risk as soon as possible, as security breaches involving personal data can cause real harm and distress to individuals.

13.2 Whilst not all security breaches have such consequences, they can still cause serious embarrassment or inconvenience to the people concerned. 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 GDPR, not just the authority as a whole.

13.3 A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. In short, there will be a personal data breach whenever any personal data is lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals. Personal data security breaches could be caused by a number of factors, including:

- deliberate or accidental action (or inaction);
- loss or theft of data or equipment on which personal information is stored;
- inappropriate access controls allowing unauthorised use of personal data;
- equipment failure;
- human error;
- unforeseen circumstances (such as fire or flood);
- hacking of ICT systems;
- 'blagging' (where information is obtained by deception);
- sending personal data to an incorrect recipient;
- alteration of personal data without permission; and
- loss of availability of personal data.

13.4 However a personal data security breach may arise or occur, there are a number of important elements to the Council's management of the incident, including containment and recovery, the assessment of the risk the incident represents and the Council's response to the breach. It is therefore important that all officers and members of the Council know how to recognise a potential breach of the security of personal data and that, if a breach is discovered or reported, that the relevant Assistant Director is informed immediately.

13.5 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 protocol is available on the intranet.

14. DOCUMENT HISTORY

14.1 The Data Protection Officer 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.

14.2 Additional information regarding this Data Protection Policy and guidance in respect of specific data protection matters can be obtained from the Data Protection Officer, who can be contacted as follows:

Data Protection Officer,
Epping Forest District Council,
Civic Offices,
High Street,
Epping,
Essex, CM16 4BZ.
☎ (01992) 564000
✉ dataprotectionofficer@eppingforestdc.gov.uk

14.3 A companion 'Guide to Data Protection', which provides further explanation of procedures for handling personal data, is available on the intranet.