EPPING TOWN COUNCIL

DATA PROTECTION POLICY 2023

Epping Town Council is fully committed to compliance with the requirements of Data Protection legislation. Epping Town Council followed the prescriptions of the Data Protection Act 1998 ("the Act"), which came into force on the 1 March 2000 and have adjusted their policies to reflect the new General Data Protection Regulation, with effect from 25th May 2018. 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 this legislation.

Introduction

We hold personal data about our employees, residents, suppliers and other individuals for a variety of Council purposes.

This policy sets out how we seek to protect personal data and ensure that Councillors and Officers understand the rules governing their use of personal data to which they have access in the course of their work. In particular, this policy requires Officers to ensure that the Data Protection Officer (DPO) be consulted before any significant new data processing activity is initiated to ensure that relevant compliance steps are addressed.

Business purposes	The purposes for which personal data may be used by us: Personnel, administrative, financial, statutory and legislative purposes, payroll, consultations and business development purposes. Council purposes include the following: Compliance with our legal, regulatory and corporate governance obligations and good practice Gathering information as part of investigations by regulatory bodies or in connection with legal proceedings or requests Ensuring Council policies are adhered to (such as policies covering email and internet use) Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of sensitive information, security vetting and checking Investigating complaints Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments Monitoring staff conduct, disciplinary matters Promoting Council services Improving services

Personal data	Information relating to identifiable individuals, such as job applicants, current and former employees, agency, contract and other staff, clients, suppliers and marketing contacts, members of the public, Council service users, residents, market traders, hirers, correspondents Personal data we gather may include: individuals' contact details, educational background, financial and pay details, details of certificates and diplomas, education and skills, marital status, nationality, job title, and CV, contact details, correspondence, emails, databases, council records
Sensitive personal data	Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings—any use of sensitive personal data should be strictly controlled in accordance with this policy.

Scope

This policy applies to all councillors and staff. You must be familiar with this policy and comply with its terms.
This policy supplements our other policies relating to internet and email use. We may supplement or amend this policy by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.
As the data controller, Epping Town Council has overall responsibility for dealing with any data breaches and determining the quality of our data protection. Council is ultimately responsible for the correct handling of its data, ensuring risks have been identified and proportionate measures taken to minimise those risks. The day to day management of data will be overseen by the Town Clerk in conjunction with staff and members.
• Please note: Council are not legally required to appoint a Data Protection Officer, but they are required to ensure they have the correct policies and procedures in place and protect all data. Council have resolved to monitor the situation regarding data breaches and appoint an independent Data Protection Officer, should they deem it necessary.

Our procedures

Fair and lawful processing:

We must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that we should not process personal data unless the individual whose details we are processing has consented to this happening.

The Data Protection Officer's responsibilities:

- Keeping the Council updated about data protection responsibilities, risks and issues

- Reviewing all data protection procedures and policies on a regular basis
- Assisting with data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from staff, council members and other stakeholders
- Responding to individuals such as members of the public, service users and employees who wish to know which data is being held on them by Epping Town Council
- Checking and approving with third parties that handle the councils data any contracts or agreement regarding data processing
  ***Please note: this will be managed by the Town Clerk as the Proper Officer of Council, in the absence of a DPO**

Responsibilities of IT support:

- Ensure all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services, such as cloud services the company is considering using to store or process data

Responsibilities of the officers:

- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection laws and the company's Data Protection Policy

The processing of all data must be:

- Necessary to deliver our services
- In our legitimate interests and not unduly prejudice the individual's privacy
- In most cases this provision will apply to routine business data processing activities.

Our Terms of Business contains a Privacy Notice relating to on data protection.

The notice:

- Sets out the purposes for which we hold personal data on customers, employees, residents and service users
- Highlights that our work may require us to give information to third parties such as expert witnesses and other professional advisers
- Provides that service users and correspondents have a right of access to the personal data that we hold about them

Sensitive personal data:

In most cases where we process sensitive personal data we will require the data subject's *explicit* consent to do this unless exceptional circumstances apply, or we are required to do this by law (e.g. to comply with legal obligations to ensure health and safety at work, comply with burial legislation and allotment legislation). Any such consent will need to

clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

Accuracy and relevance:

We will ensure that any personal data we process is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. We will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.
Individuals may ask that we correct inaccurate personal data relating to them. If you believe that information is inaccurate you should record the fact that the accuracy of the information is disputed and inform the DPO [Epping Town Council office].

Your personal data:

You must take reasonable steps to ensure that personal data we hold about you is accurate and updated as required. For example, if your personal circumstances change, please inform the Data Protection Officer so that they can update your records.

Data security:

You must keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

Storing data securely:

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it
- Printed data should be shredded when it is no longer needed
- Data stored on a computer should be protected by strong passwords that are changed regularly. We encourage all staff to use a password manager to create and store their passwords.
- Data stored on CDs or memory sticks must be locked away securely when they are not being used
- The DPO must approve any cloud used to store data
- Servers containing personal data must be kept in a secure location, away from general office space
- Data should be regularly backed up in line with the company's backup procedures
- Data should never be saved directly to mobile devices such as laptops, tablets or smartphones
- All servers containing sensitive data must be approved and protected by security software and strong firewall.

Data retention:

We must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons that the personal data was obtained, but should be determined in a manner consistent with our data retention guidelines.

Subject access requests:

Please note that under the Data Protection Act 1998, individuals are entitled, subject to certain exceptions, to request access to information held about them. Epping Town Council have a Subject Access Request Policy and Form to process any subject access requests (2019). If you receive a subject access request, you should refer that request immediately to the DPO.

Please contact the Data Protection Officer if you would like to correct or request information that we hold about you. There are also restrictions on the information to which you are entitled under applicable law. The DPO will advise on this.

Processing information in accordance with an individual's rights:

You should abide by any request from an individual not to use their personal data for direct marketing purposes and notify the DPO about any such request.
Do not send direct marketing material to someone electronically (e.g. via email) unless you have an existing business relationship with them in relation to the services being marketed.
Please contact the DPO for advice on direct marketing before starting any new direct marketing activity.
Epping Town Council will only use data for the purposes of Council business.

Training:

All staff will receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided at least every two years or whenever there is a substantial change in the law or our policy and procedure **Training is provided in-house when needed.** New councillors will also receive Data Protection training.

It will cover:

- **The law relating to data protection**
- **Our data protection and related policies and procedures.**

Completion of training is compulsory.

GDPR and Data Protection Act provisions:

Where not specified previously in this policy, the following provisions will be in effect on or before 25 May 2018.

Privacy Notice – transparency of data protection:

Being transparent and providing accessible information to individuals about how we will use their personal data is important for our organisation. The following are details on how we collect data and what we will do with it:

Conditions for processing:

We will ensure any use of personal data is justified using at least one of the conditions for processing and this will be specifically documented. All staff who are responsible for processing personal data will be aware of the conditions for processing. The conditions for processing will be available to data subjects in the form of a privacy notice.

Justification for personal data:
We will process personal data in compliance with all six data protection principles.
We will document the additional justification for the processing of sensitive data, and will ensure any biometric and genetic data is considered sensitive.

Consent:
The data that we collect is subject to active consent by the data subject. This consent can be revoked at any time.

Criminal record checks:
Any criminal record checks are justified by law. Criminal record checks cannot be undertaken based solely on the consent of the subject.

Data portability:
Upon request, a data subject should have the right to receive a copy of their data in a structured format. These requests should be processed within one month, provided there is no undue burden and it does not compromise the privacy of other individuals. A data subject may also request that their data is transferred directly to another system. This must be done for free.

Right to be forgotten:
A data subject may request that any information held on them is deleted or removed, and any third parties who process or use that data must also comply with the request. An erasure request can only be refused if an exemption applies. Please note: some data must be kept in accordance with other laws, such as cemetery records, personnel records and accident records.

Privacy by design and default:
Privacy by design is an approach to projects that promote privacy and data protection compliance from the start. The DPO will be responsible for conducting Privacy Impact Assessments and ensuring that all IT projects commence with a privacy plan.
When relevant, and when it does not have a negative impact on the data subject, privacy settings will be set to the most private by default.

International data transfers:
No data may be transferred outside of the EEA without first discussing it with the data protection officer. Specific consent from the data subject must be obtained prior to transferring their data outside the EEA.

Data audit and register:
Regular data audits to manage and mitigate risks will inform the data register. This contains information on what data is held, where it is stored, how it is used, who is responsible and any further regulations or retention timescales that may be relevant.

Sharing of data:
Sharing of data with any third parties is not permitted without the express permission in writing of the data subject. Extreme caution should be taken with all data sharing.

Reporting breaches:

All members of staff have an obligation to report actual or potential data protection compliance failures. Data breaches **MUST** be reported to the Town Clerk as soon as they become apparent. This allows us to:

- Investigate the failure and take remedial steps if necessary
- Follow the Data Breach Procedure
- Maintain a register of Compliance Failures
- Notify the Information Commissioner's Office (ICO) of any compliance failures that are material either in their own right or as part of a pattern of failures

Please refer to our Compliance Failure Policy for our reporting procedure.

Monitoring:

Everyone must observe this policy. The DPO has overall responsibility for this policy. They will monitor it regularly to make sure it is being adhered to.

Compliance:

It is extremely important that everyone holding data in relation to the operations of Epping Town Council complies with this policy.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the DPO. ***Please note:** In the absence of a DPO, this is the Town Clerk as the Proper Officer of the Council.

What information is being collected?	
Who is collecting it?	
How is it collected?	
Why is it being collected?	
How will it be used?	
Who will it be shared with?	
Identity and contact details of any data controllers	
Details of transfers to third country and safeguards	
Retention period	

Approved: March 2023
Next review: Feb 2025