Data Protection Policy

Felixstowe Town Council is committed to being transparent about how it collects and uses the personal data of its workforce, and to meeting its data protection obligations. This policy sets out the Council`s commitment to data protection, and individual rights and obligations in relation to personal data.
Council hold personal data about its 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.

Definitions

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, who must be familiar with this policy and comply with its terms.

This policy supplements our other policies relating to internet, email use and data protection section of the Employee Handbook. This policy may supplemented or amended by additional policies and guidelines from time to time. Any new or modified policy will be circulated to staff before being adopted.

Who is responsible for this policy?

Felixstowe Town Council as the Data Controller has overall responsibility for the day-to-day implementation of this policy.

Oversight is provided by the Council's nominated DPO, the Local Council Public Advisory.

Procedures

Fair and lawful processing

Council 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 Felixstowe Town Council
- Checking and approving with third parties that handle the council's data any contracts or agreement regarding data processing

Responsibilities of the IT Manager

- 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 Council is considering using to store or process data, to ensure that such third-parties have appropriate technical security measures in place to safeguard any personal data processed by them

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 this Data Protection Policy
- to access only data that authorisation to access has been received and only for authorised purposes;
- not to disclose data except to individuals (whether inside or outside the organisation) who have appropriate authorisation;
- not to remove personal data, or devices containing or that can be used to access personal data, from Council's premises without adopting appropriate security measures (such as encryption or password protection) to secure the data and the device;
- not to store personal data on local drives or on personal devices that are used for work purposes;

The processing of all data must be:

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

Council's Website provides a Privacy Notice relating to data protection, a copy of which can also be obtained from the Town Hall.

The notice:

- Sets out the purposes for which Council hold personal data on customers, employees, residents and service users
- Highlights that Council's work may require information to be given 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 Council processes sensitive personal data Council will require the data subject's explicit consent to do this unless exceptional circumstances apply, or Council 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
Council will ensure that any personal data that it processes is accurate, adequate, relevant and not excessive, given the purpose for which it was obtained. Council 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 Council corrects inaccurate personal data relating to them. If it is believed that information is inaccurate the fact should be recorded that the accuracy of the information is disputed and the DPO, the Local Council Public Advisory Service should be informed.

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 Town Council so we can update your records.

Data security
Personal data must be kept secure against loss or misuse. Where other organisations process personal data as a service on Council's 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. A password manager should be considered to create and store passwords.
- Data should not be stored on CDs, memory sticks or removable media, unless in accordance with Council's backup procedures.
- 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 council'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
Council 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 Council's data retention policy.

Subject Access requests

Under the UK Data Protection Act 2018, individuals are entitled, subject to certain exceptions, to request access to information held about them.

Any subject access request received will be immediately referred to the DPO, who may ask Officers and Councillors to help comply with those requests.

Please contact the Town Council if you would like to correct or request information that Council holds about you. There are also restrictions on the information to which an individual is entitled under applicable law.

Processing data in accordance with the individual's rights
Council 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.

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 Council's policy and procedure.

Training is provided through an in-house seminar on a regular basis.

It will cover:

- The law relating to data protection
- Council's data protection and related policies and procedures.

Individuals whose roles require regular access to personal data, or who are responsible for implementing this policy or responding to subject access requests under this policy, will receive additional training to help them understand their duties and how to comply with them.

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 Council will use individual's personal data is important for our organisation.

Conditions for processing

Council 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

Council will process personal data in compliance with the following six data protection principles:

- Council processes personal data lawfully, fairly and in a transparent manner.
- Council collects personal data only for specified, explicit and legitimate purposes.
- Council processes personal data only where it is adequate, relevant and limited to what is necessary for the purposes of processing.
- Council keeps accurate personal data and takes all reasonable steps to ensure that inaccurate personal data is rectified or deleted without delay.
- Council keeps personal data only for the period necessary for processing.

- Council adopts appropriate measures to make sure that personal data is secure, and protected against unauthorised or unlawful processing, and accidental loss, destruction or damage.

Council 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 Council collects 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.

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.

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.

Reporting breaches
All members of staff have an obligation to report actual or potential data protection compliance failures. This allows Council to:

- Investigate the failure and take remedial steps if necessary
- Maintain a register of compliance failures
- Notify the Supervisory Authority (SA) of any compliance failures that are material either in their own right or as part of a pattern of failures within 72 hours of discovery.
- To report a breach, please contact the Town Clerk via townclerk@felixstowe.gov.uk

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.

Consequences of failing to comply

Compliance with this policy is taken very seriously. Failure to comply puts both the individual (Councillor or Officer) and the Council at risk. The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under Council's procedures which may result in dismissal.

If you have any questions or concerns about anything in this policy, do not hesitate to contact the Town Clerk tel: 01394 282086 Email: townclerk@felixstowe.gov.uk