



# WESTGATE-ON-SEA TOWN COUNCIL DATA PROTECTION POLICY ADOPTED 27.05.2020

## Policy Statement

The Town Council has a duty to comply with the 2018 General Data Protection Regulations. The General Data Protection Regulations retain the existing legal principles of the 1998 Data Protection Act and adds some additional protections as to how personal data and sensitive personal data can be collected, handled, and used. The GDPR 2018 says that the information provided to people about how we process their personal data must be concise, transparent, intelligible, and easily accessible, written in clear and plain language. The Town Council is committed to ensure high standards of practice are maintained when handling personal information concerning employees, Councillors and the public either electronically or on paper.

The Town Council is open and transparent about its operations and works closely with the community. Details of information which is readily available is contained in the Council's Publication Scheme.

The underlying principles which the Town Council will comply with, about personal data include:

- **It is processed fairly and lawfully** – this means that information should only be collected from individuals if staff and Councillors have been open and honest about why they want the information.
- **It is processed for specified purposes only.**
- **It is relevant to what it is needed for** – data will be monitored so that too much or too little is not kept; only data that is needed should be held.
- **It is accurate and kept up to date** – personal data should be accurate, if it is not it should be corrected.
- **It is not kept longer than it is needed.**
- **It is processed in accordance with the rights of individuals** – this means that individuals must be informed, upon request, of all the information held about them.
- **It is kept securely** – this means that only staff and Councillors can access the data, it should be stored securely so it cannot be accessed by members of the public.

The Council will ensure that at least one of the following six lawful bases for processing personal data are met:

- **Consent** – able to demonstrate consent was given in written declaration
- **Legitimate interests** – the privacy policy of a controller must inform data subjects about the legitimate interests that are the basis for the balancing of interests.
- **Contractual necessity** – personal data may be processed if the processing is necessary in order to enter into or perform a contract with the data subject.
- **Compliance with legal obligation** – personal data may be processed if the controller is legally required to perform such processing, for example complying with the requirements of legislation.
- **Vital interests** – personal data may be processed to protect the “vital interests” of the data subject, for example in a life and death situation it is permissible to use a person's emergency

contact information without their consent.

- **Public interest** – personal data may be processed if the processing is necessary for the performance of tasks carried out by a public authority or private organisation acting in the public interest.

### **Disclosure of Information**

If an elected Member of the Council needs to access information to help carry out their duties, this is acceptable. They are only able to access as much information as necessary and it should only be used for that specific purpose. If for instance someone has made a complaint about speeding vehicles, a Councillor may access an address and telephone number of the person who has made the complaint so they can help with the enquiry. However, before they access any sensitive information about a person, they would need consent to do this from the Town Clerk, who in turn would seek consent from the data subject. Data should never be used for political reasons unless the data subjects have consented.

### **Confidentiality**

The Town Council staff must be aware that when complaints or queries are made, they must remain confidential unless the subject gives permission otherwise. When handling personal data, this must also remain confidential. If a data breach is identified the ICO must be informed within 72 hours and an investigation will be conducted.

### **Data Protection and Employees**

- The Act applies to the monitoring of employees for example: To detect excessive use of telephone calls, private emails, and internet use via the Council's resources.
- The Council will only seek to collect information concerning an employee's health with the employee's consent. Once collected this information will be held securely and with limited access to the information. The Council will only collect justified information.

### **Employees Right To Access Information**

- The Council's employees have a legal right to access information held by the Council, which includes any information regarding any grievances or disciplinary action, and information gathered through monitoring processes.

### **Application of Policy**

- This policy applies to all Council employees, Councillors, contractors, and members of the public

### **Data Control**

- The Town Clerk is the Council's Data Controller.

### **Contact Details**

Please contact us if you have any questions about our Privacy Notice or the personal data we hold about you or to exercise all relevant rights, queries or complaints to: The Data Controller, Westgate-on-Sea Town Council, 78 St Mildreds Road, Westgate-on-Sea, CT8 8RF. Telephone 01843 836182, email [townclerk@westgateonseas.gov.uk](mailto:townclerk@westgateonseas.gov.uk).

This policy will be reviewed as part of the annual review of compliance and effectiveness of the policy.