



Wivenhoe Town Council

Data Protection Policy

General rules in complying with the Data Protection Act

Policy points are numbered. The numbering corresponds to explanations of 'why?' and 'how?' for each point further down the page.

What must I do?

1. **MUST:** All staff, members and volunteers must **comply** with the requirements of the Data Protection Act and Article 8 of the Human Rights Act when handling personal data of natural individuals; whether relating to members of the public or other ECC staff.
2. **MUST:** All staff, members and volunteers must collect, hold and use the **minimum** personal data necessary to deliver our services
3. **MUST:** All staff must take reasonable steps to ensure the data we hold is **accurate**, up to date and not misleading.
4. **MUST:** Consent must be obtained if personal data is to be used for **promoting** or marketing goods and services.
5. **MUST:** All managers must ensure that the personal data they manage is reviewed regularly and **destroyed** when no longer required.
6. **MUST:** If you receive a **request** from a member of the public or a member of staff asking to access their personal information, you must handle it in accordance with the FOI Policy
7. **MUST:** If you receive a request from anyone asking to access the personal information of **someone other than themselves**, you must handle it in accordance with the Freedom of Information Requests regulations or the Environmental Information Regulations Requests regulations.
8. **MUST:** If someone contacts WTC formally stating that their personal data on our records is **inaccurate**, the request should be fully considered and the record amended if the request is valid.
9. **MUST:** You must follow system user **guidance** or other formal processes which are in place to ensure that only those with a business need to access personal data are able to do so
10. **MUST:** Information must only be shared with external organisations if it is done under a formal **Information Sharing Protocol** which clearly explains the limits of what can be shared and what safeguards will be in place.

11. **MUST:** All staff and elected members must be **trained** to an appropriate level, based on their roles and responsibilities, to be able to handle personal data securely.
12. **MUST NOT:** You must not access personal data which you have **no right to view**
13. **MUST NOT:** You must not **share** any personal data held by ECC with an individual or organisation based in any country outside of the European Economic Area (European Union member states plus Iceland, Liechtenstein and Norway).

Why must I do it?

1. To comply with UK legislation
2. To comply with the 'minimisation principle' in Data Protection Act 2018. You must only collect and/or hold the minimum amount of information you need to carry out our business purpose. It is not acceptable to hold information on the basis that it might possibly be useful in the future without a view of how it will be used. Changes in circumstances or failure to keep the information up to date may mean that information that was originally adequate becomes inadequate.
3. To comply with the Data Protection Act 2018.
4. To comply with the principles of the Data Protection Act 2018
5. To comply with the principles of the Data Protection Act. If information is kept for longer than necessary then it may be both irrelevant and excessive.
6. To comply with the Subject Access provisions of the Data Protection Act 2018.
7. To comply with the Data Protection Act 2018, the Freedom of Information Act and the Environmental Information Regulations
8. To comply with the principles of the Data Protection Act 2018.
9. To comply with the principles of the Data Protection Act 2018.
10. To comply with the Data Protection Act 2018.
11. To comply with this policy.
12. To comply with the Data Protection Act 2018
13. To comply with the principles of the Data Protection Act. The member states of the EEA share common legislation which provides assurance to us that personal data will be securely handled under the same provisions that exist under the Data Protection Act.

How must I do it?

1. By following the points in this policy
2. By ensuring that the means you use to gather personal data (such as forms etc) only ask for the information that is required in order to deliver the service.
3. By considering that anything committed to record about an individual may be accessible by that individual in the future
4. You must review personal data regularly and delete information which is no longer required, although you must take account of statutory and recommended minimum retention periods. Subject to certain conditions, the Act allows us to keep indefinitely personal data processed only for historical, statistical or research purposes.
5. By completing compulsory training courses relevant to your role

6. To update ROPA when any change to the purposes of processing personal data occur
7. By being aware through training and guidance on what information is appropriate for you to access to do your job

References

Data Protection Act 2018

Human Rights Act 1998

Lawful Business Practice Regulations 2000

ICO: Employment Practices Code and Supplementary Guidance

Reviewed 23 February 2026 F&P Committee

Next Review Date February 2027