Data Protection Policy

Adopted Date:	10 December 2018
Policy Reviewed:	12 March 2026
Next Review Date:	12 March 2027

1. Introduction

1.1 Ilfracombe Town Council has a responsibility under Data Protection Act 2018 to hold, obtain, record, use and store all personal data relating to an identifiable individual in a secure and confidential manner. This policy is a statement of what the Town Council does to ensure its compliance with the Act.

1.2 The Data Protection Policy applies to all Ilfracombe Town Council employees, councillors, volunteers and contractors. The Policy provides a framework within which the Town Council will ensure compliance with the requirements of the Act and will underpin any operational procedures and activities connected with the implementation of the Act.

2. Background

2.1 The Data Protection Act 2018 governs the handling of personal information that identifies living individuals directly or indirectly and covers both manual and computerised information. It provides a mechanism by which individuals about whom data is held (the "data subjects") can have a certain amount of control over the way in which it is handled.

2.2 Some of the main features of the Act are:

- All data covered by the Act must be handled in accordance with the Seven Data Protection Principles (see Appendix 1)

- The person about whom the information is held (the Data Subject) has various rights under the Act including the right to be informed about what personal data is being processed, the right to request access to that information, the right to request that inaccuracies or incomplete data are rectified, and the right to have personal data erased and to prevent or restrict processing in specific circumstances. Individuals also have the right to object to processing based on the performance of a task in the public interest/exercise of official authority (including profiling), direct marketing (including profiling); and processing for the purposes of scientific/historical research and statistics. There are also rights concerning automated decision making (including profiling) and data portability.

- Processing of special categories of data must be done under a lawful basis. This data includes information about race, ethnic origin, political persuasion, religious belief, trade union membership, genetics, biometrics (where used for identification purposes), health, sex life and sexual orientation.

- The Data Protection Act deals with criminal offence data in a similar way to special category data and sets out specific conditions providing lawful authority for processing it.

- There is a principle of accountability of data controllers to implement appropriate technical and organisational measures that include internal data protection policies and procedures, staff training and awareness of the requirements of the Act, internal audits of processing activities, appointing a data protection officer, and implementing measures that meet the principles of data protection by design and data protection by default, including data minimisation, transparency, and creating and improving security features on an ongoing basis.

- Data protection impact assessments are carried out where appropriate as part of the design and planning of projects, systems and programmes.

- Data controllers must have written contracts in place with all data processors and ensure that processors are only appointed if they can provide 'sufficient guarantees' that the requirements of the Act will be met and the rights of data subjects protected.

- Data breaches that are likely to result in a risk to the rights and freedoms of individuals must be reported to the Information Commissioner's Office within 72 hours of the Council becoming aware of such breach. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the Council will notify those individuals concerned directly.

- The Information Commissioner is responsible for regulation and issue notices to organisations where they are not complying with the requirements of the Act. The Information Commissioner also had the ability to prosecute those who commit offences under the Act and to issue fines.

3. Policy Statement

3.1 The Town Council is committed to ensuring that personal information is handled in a secure and confidential manner in accordance with its obligations under the Data Protection Act 2018 and professional guidelines. The Town Council will use all appropriate and necessary means at its disposal to comply with the Data Protection Act and associated guidance.

4. Roles and Responsibilities

4.1 Data Protection Officer

4.1.1 The Town Council is not a public authority for the purposes of GDPR (section 7(3) of the DPA 2018) and therefore does not need to appoint a Data Protection Officer.

4.2 Town Council

4.2.1 Informing and advising any processor engaged by the Town Council as data controller and any employee of the Town Council who carries out processing of personal data, of that person's obligations under the legislation.

4.2.2 Ensuring that the organisation complies with its responsibilities under the Data Protection Act through monitoring of activities and incidents. The Town Council will also ensure that there are adequate resources to support the work outlined in this policy to ensure compliance with the Data Protection Act.

4.3 Proper Officer/Town Clerk

4.3.1 The Proper Officer/Town Clerk (or Responsible Financial Officer where appropriate) is responsible for the operational implementation of this policy and for ensuring that staff and councillors are aware of their data protection responsibilities.

4.4 All Staff and Councillors

4.4.1 All staff and Councillors will ensure that:

- Personal information is treated in a confidential manner in accordance with this and any associated policies.
- The rights of data subjects are respected at all times.
- Privacy notices will be made available to inform individuals how their data is being processed.
- Personal information is only used for the stated purpose, unless explicit consent has been given by the Data Subject to use their information for a different purpose.
- Personal information is only disclosed on a strict need to know basis, to recipients who are entitled to that information.
- Personal information held within applications, systems, personal or shared drives is only accessed in order to carry out work responsibilities.
- Personal information is recorded accurately and is kept up to date.

It is the responsibility of all staff and Councillors to ensure that they comply with the requirements of this policy and any associated polices or procedures.

4.5 Contractors and Employment Agencies

4.5.1 Where contractors are used, the contracts between the Town Council and these third parties should contain mandatory information assurance clauses to ensure that the contract staff are bound by the same code of behaviour as Town Council members of staff and Councillors in relation to the Data Protection Act.

4.6 Volunteers

4.6.1 All volunteers are bound by the same code of behaviour as Town Council members of staff and Councillors in relation to the Data Protection Act.

5. Records Management

5.1 Good records management practice plays a pivotal role in ensuring that the Town Council is able to meet its obligations to provide information, and to retain it, in a timely and effective manner in order to meet the requirements of the Act. All records should be retained and disposed of in accordance with the Town Council retention schedule.

6. Consent

6.1 The Town Council will take all reasonable steps to ensure that service users, members of staff, volunteers, and contractors are informed of the reasons the Town Council requires information from them, how that information will be used and

who it will be shared with. This will enable the data subject to give explicit informed consent to the Town Council handling their data where legal basis for processing is consent.

6.2 Should the Town Council wish to use personal data for any purpose other than that specified when it was originally obtained, the data subject's explicit consent should be obtained prior to using the data in a new way unless exceptionally such use is in accordance with other provisions of the Act.

6.3 Should the Town Council wish to share personal data with anyone other than those recipients specified at the time the data was originally obtained, the data subject's explicit consent should be obtained prior to sharing that data, failure to do so could result in a breach of confidentiality.

7. Accuracy and Data Quality

7.1 The Town Council will ensure that all reasonable steps are taken to confirm the validity of personal information directly with the data subject.

7.2 All members of staff and Councillors must ensure that service user personal information is checked and kept accurate and up to date on a regular basis, for example, by checking it with the service user when they attend for appointments in order that the information held can be validated.

7.3 Where a member of the public exercises their right for their data to be erased, rectified, or restricted, or where a member of the public objects to the processing of their data, the appropriate procedures must be followed.

8. Data Protection Impact Assessments

8.1 A data protection impact assessment is a process which helps to assess privacy risks to individuals in the collection, use and disclosure of information. They must be carried out at the early stages of projects and are embedded into the Town Council's decision-making process.

9. Providers

9.1 The Town Council must have written contracts in place with all suppliers who process personal data on behalf of the Town Council as "data processors". The Town Council will ensure that processors are only appointed if they can provide 'sufficient guarantees' through the procurement process that the requirements of the Act will be met and the rights of data subjects protected.

10. Complaints

10.1 Any expression of dissatisfaction from an applicant with reference to the Town Council's handling of personal information will be treated as a complaint and handled under the Town Council's complaint's processes.

10.2 Should the complainant remain dissatisfied with their complaint to the Council; a complaint can be made to the Information Commissioner's Office who will then investigate the complaint and take action where necessary.

11. Security and Confidentiality

11.1 All staff and Councillors must ensure that information relating to identifiable individuals is kept secure and confidential at all times. The Town Council will ensure that its holdings of personal data are properly secured from loss or corruption and that no unauthorised disclosures of personal data are made.

11.2 Personal data will not normally be transferred outside the United Kingdom. Where transfers outside the UK are necessary, the Council will ensure that appropriate safeguards are in place in accordance with UK GDPR and the Data Protection Act 2018.

12. Rights of Data Subjects

12.1 Individuals wishing to request their information as a Subject Access Request (SAR) should contact the Town Council, who will arrange for the information to be processed in accordance with the Data Protection Act. Subject Access Requests will normally be responded to **within one calendar month**, in accordance with UK GDPR. This period may be extended by a further two months where requests are complex or numerous.

12.2 Individuals should also make requests in writing to the Town Council if they wish to exercise their other rights under the legislation.

13. Policy Review

13.1 This policy will be reviewed every year or sooner if legislation or guidance from the Information Commissioner's Office requires it.

Appendix 1:

Seven Principles of UK GDPR

Lawfulness, fairness and transparency – data must be processed legally, fairly and in a transparent manner in relation to individuals.

Purpose limitation – Data must be 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.

Data minimisation – Data collected must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Accuracy – Data must be 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.

Storage limitation – Data should only be 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.

Integrity and confidentiality (security) – Data must be 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.

Accountability – The data controller shall be responsible for, and be able to demonstrate compliance with all the above principles.