



INGLEBY BARWICK TOWN COUNCIL

DATA PROTECTION POLICY

1.0 INTRODUCTION

- 1.1 Ingleby Barwick Town Council is fully committed to compliance with the requirements of the Data Protection Act 1998 which came into force on the 1st March 2000, (“the Act”), and the General Data Protection Regulations 2014 (GDPR).
- 1.2 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 the Act.

2.0 STATEMENT OF POLICY

- 2.1 In order to operate efficiently, the Town Council has to collect and use information about people with whom it works. These may include members of the public, current, past and prospective employees, and suppliers. In addition, it may be required by law to collect and use information to comply with the requirements of central government. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it be on paper, in computer records or recorded by any other means; there are safeguards within the Act to ensure this.
- 2.2 The Town Council regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the Council and those with whom it carries out business. The Council will ensure it treats personal information lawfully and correctly. To this end the Council fully endorses and adheres to the Principles of Data Protection as set out in the Data Protection Act 1998.

3.0 THE PRINCIPLES OF DATA PROTECTION

- 3.1 The Act stipulates that anyone processing personal data must comply with **Eight Principles** of good practice. These Principles are legally enforceable.
- 3.2 The Principles require that personal information:
- I. Shall be processed fairly and lawfully and in particular, shall not be processed unless specific conditions are met
 - II. Shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes
 - III. Shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed
 - IV. Shall be accurate and where necessary, kept up to date
 - V. Shall not be kept for longer than is necessary for that purpose or those purposes
 - VI. Shall be processed in accordance with the rights of data subjects under the Act
 - VII. Shall be kept secure i.e. protected by an appropriate degree of security
 - VIII. Shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.
- 3.3 The Act provides conditions for the processing of any personal data. It also makes a distinction between **personal data** and “**sensitive**” **personal data**.

4.0 DEFINITIONS

- 4.1 Personal data is defined as data relating to a living individual, who can be identified from:
- That data
 - That data and other information which is in the possession of, or is likely to come into the possession of, the data controller and includes an expression of opinion about the individual and any indication of the intentions of the data controller, or any other person in respect of the individual.
- 4.2 Sensitive personal data is defined as personal data consisting of information as to:
- Racial or ethnic origin
 - Political opinion
 - Religious or other beliefs
 - Trade union membership
 - Physical or mental health or condition
 - Sexual life
 - Criminal proceedings or convictions.
- 4.3 A data controller is defined as any person (or organisation) with regard to particular personal data, including decisions regarding the purposes for which personal data are processed and the way in which it is processed.
- 4.4 A data subject is defined as any living individual who is the subject of personal information held by an organization.
- 4.5 Processing is defined as any operation related to organisation, retrieval, disclosure and deletion of data and includes:
- Obtaining and recording data
 - Accessing
 - Altering
 - Adding to
 - Merging
 - Deleting data
 - Retrieval
 - Consultation or use of data
 - Disclosure or otherwise making data available.
- 4.6 Third party is defined as any individual/organization other than the data subject, the data controller or its agents.

5.0 HANDLING OF PERSONAL/SENSITIVE INFORMATION

- 5.1 The Town Council will, through appropriate management and the use of criteria and controls:
- Observe fully conditions regarding the fair collection and use of personal information
 - Meet its legal obligations to specify the purpose for which information is used
 - Collect and process appropriate information and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements
 - Ensure the quality of information used
 - Apply checks to determine the length of time information is held
 - Take appropriate measures to safeguard personal information
 - Ensure that the rights of people about whom the information is held can be fully exercised under the Act.
- 5.2 These include:
- The right to be informed that processing is being undertaken
 - The right of access to one's personal information within the statutory 40 days
 - The right to correct, rectify, block or erase information regarded as wrong information.

6.0 IMPLEMENTATION

6.1 The Clerk to Ingleby Barwick Town Council is responsible for ensuring adherence with the Data Protection Act.

7.0 NOTIFICATION TO THE INFORMATION COMMISSIONER

7.1 The Information Commissioner maintains a public register of data controllers. The Town Council is registered as such.

7.2 The Data Protection Act 1998 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence. The Clerk will review the Data Protection/Records Management Register annually, prior to notification to the Information Commissioner.

7.3 Any changes to the register must be notified to the Information Commissioner, within 28 days. To this end, any changes required between annual reviews will be brought to the attention of the Clerk immediately, who will then inform the Information Commissioner.

8.0 RECORDS MANAGEMENT

8.1 Ingleby Barwick Town Council recognises the efficient management of its records is necessary in order to comply with its legal and regulatory obligations and to contribute to the effective overall management of the Town Council. This document provides the framework through which this effective management can be achieved and audited.

8.2 The Town Council seeks to make standard management and operational documents, minutes, agendas, financial information, latest news and reports available on the Council website:
www.inglebybarwicktowncouncil.org.uk

9.0 SCOPE OF THE POLICY

9.1 This policy applies to all records created, received or maintained by the Town Council, its Members, staff, contractors or volunteers, whilst carrying out its functions.

9.2 Records are defined as all those documents that facilitate the business carried out by the Town Council and which are thereafter retained (for a set period) to provide evidence of its transactions or activities. These records may be created, received, or maintained in hard copy or electronically.

9.3 Emails will be purged regularly and deleted safely.

9.4 A small percentage of the Town Council's records will be selected for permanent preservation as part of the Council's archives and for historical research and interest.

10.0 RESPONSIBILITIES

10.1 The Town Council has a corporate responsibility to maintain its records and record management systems in accordance with the regulatory environment.

10.2 The person with overall responsibility for this Policy is the Town Clerk (Proper Officer). Only the staff can directly access the data, which is held securely by a system of passwords; it cannot be accessed by members of the public.

10.3 Ingleby Barwick Town Council may hold personal information about individuals such as their addresses, emails, and telephone numbers. This is securely kept at the office of the Town Council and is not available for public access. All data stored on the Council's computers is password protected.

10.4 Once data falls outside the minimum retention time of Council's document retention policy, it will be shredded or securely deleted from the Computer.

11.0 DATA RECEIVED AND CREATED BY TOWN COUNCILLORS

11.1 All data received and created by Councillors acting on behalf of the Town Council and in their role as an elected member is subject to the Data Protection Act 1998 and Freedom of Information Act 2000.

11.2 It is recognised that members of the public may contact Ingleby Barwick Town Councillors directly through email or letter from time to time. Councillors should:

- Forward the email or letter to the Town Clerk to respond to and delete any electronic copy from their system; or
- Respond to the email or letter directly and provide a copy to the Clerk for the formal record.

11.3 If Councillors retain personal information either in paper format or electronically about individuals such as their addresses, emails, and telephone numbers when acting on behalf of members of the public and local organisations, it is recommended they seek advice from the Commissioner's Office.

11.4 It is the responsibility of the Town Councillor, if in doubt, to seek clarification from the Commissioner's Office helpline to establish whether they should apply for individual registration.

11.5 It is safest for Councillors to delete any correspondence once a matter has come to a natural conclusion rather than hold the information indefinitely. If you believe the correspondence is important historically to the Town Council, then a copy should be forwarded to the Clerk clearly marked for the 'formal record' and it will be kept accordingly.

12.0 RETENTION OF DOCUMENTS OR ELECTRONIC DATA

12.1 The Town Council is required to maintain a retention schedule. There is a clear need to retain documentation for audit purposes, staff management, tax liabilities, and the eventuality of legal disputes and legal proceedings. The schedule lays down the minimum length of time which the records need to be retained for audit and other purposes and the action which should be taken when it is of no further administrative use. Additional documents are also identified, in the Records Management and Security Policy, which are not subject to audit, staff management, tax liabilities and other purposes, but for the general management of the Town Council or of historical interest.

12.2 The retention refers to records regardless of the media in which they are stored.

12.3 The Retention Schedule may be found as Appendix A of the Records Management and Security Policy.

13.0 DISCLOSURE OF PERSONAL INFORMATION

13.1 If an elected member of the Council needs to obtain personal information to help carry out their duties, this is acceptable. They are only able to obtain as much personal information as necessary and it should only be used for the specific purpose. If, for instance, someone has made a complaint about over hanging bushes in a garden, the Clerk may give a Councillor or the appropriate local authority the address and telephone number of the person who has made the complaint, so they can help with the enquiry. A Councillor may only do this providing they represent the area in which the subject lives. Data should never be used for political reasons unless the data subjects have consented.

14.0 OTHER DOCUMENTS INCLUDING WRITTEN NOTES OF THE CLERK AND COUNCILLORS

14.1 The Clerk's handwritten notes of Town Council meetings are routinely destroyed once the minutes have been approved. Other handwritten notes held by Councillors or the Clerk, from conferences and other Town Council related events, when no longer relevant or required will be destroyed.

14.2 Information from other bodies, e.g. planning applications, circulars, etc. from Stockton Borough Council, CALC, NALC, TVRCC, etc. Such information should be retained for as long as it is useful and relevant and then destroyed.

15.0 DOCUMENTATION RELATING TO STAFF/PERSONAL INFORMATION

15.1 Staff/personal information should be kept securely and in accordance with the Eight Data Protection Principles contained in the Data Protection Act 1998 (see Clause 3.2 of this policy). The principles provide that personal data in relation to staff should not be kept for longer than is necessary for the purpose it was held. However, after an employment relationship has ended, the Town Council will need to retain and access staff records for former staff for the purposes of giving references, payment of tax, national insurance contributions and pensions, and in respect of any related legal claims made against the Town Council.

16.0 PUBLIC RIGHT OF ACCESS TO INFORMATION

16.1 Under the Freedom of Information Act, 2000, which came into force on 1st January 2005, everyone has a right to know what information is held by the Town Council and why, personal or non-personal, with certain exemptions. The Town Council uses the model Freedom of Information Publication Scheme, which identifies what information the Town Council routinely makes available, and the cost of providing this.

16.2 The Town Council will, through the Clerk, meet any request for information made in writing, in legible form capable of being used for subsequent reference, within **20 working days** of receipt of the request, unless the provision of such information is deemed not to be in the public interest, or is commercially sensitive, or already in the public domain, or is information about a third party. The Town Council is entitled if they so wish, to request a fee for the provision of information requested under the Freedom of Information Act. This fee will never be more than the actual cost of providing the information, which includes staff time, stationery, postage and printing costs, and will be no more than a maximum of £10.00.

16.3 Where an applicant specifically requests information about a third party, the request falls within the remit of the Freedom of Information Act. However, the Town Council must apply the Data Protection Principles when considering disclosure of information relating to living individuals. The Town Council must not release third party information, if to do so would breach these Principles

16.4 The Town Council maintains the right not to respond to repeated or vexatious requests, e.g. when there has already been an identical request made by the applicant to which the Town Council has responded.

16.5 An applicant denied access to information must be given the reason for refusal and may appeal to the Information Commissioner.

17.0 FEES

17.1 A charge will be made for the photocopying of any information requested, at 5p per sheet.

17.2 A charge of £10.00 will be made for a request for an applicant's personal information, such fee being payable in advance.

17.3 The applicant has up to 3 months to make payment; only on receipt of payment will the Town Council authorise the release of information. Should payment not be received within this time limit, the request will be declared void.