Yarm Town Council

Data Protection Policy

27th April 2023

Contents

Foreword

This policy was agreed and adopted by the Town Council.

Yarm Town Council policy documents are reviewed from time to time and new editions may be issued. Users should ensure they have the latest copy by referring to the version on the Town Council Website.

Compliance with this policy does not confer immunity from prosecution for breach of statutory obligations.

Requirements

In this policy:

Must: Indicates a mandatory requirement.

Should: Indicates best practice and the preferred option. Reasonable justification must be provided for any alternative action.

Data Protection Policy

1. Introduction

1.1 Yarm 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. 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. The Act – Data Protection Act 2018

3.1 The protection of personal information about living individuals is a requirement of law. The Data Protection Act 2018's full provisions came into force on the 25th May 2018. The Act is designed to incorporate and build upon the requirements of the 1998 Act which made provision for the regulation of processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information. The Data Protection Act 2018 has made best practice a legal requirement. It obliges organisations to provide transparency on their data processing methods and restore individuals' sense of control over their personal data

3.2 The Act places obligations on those who record and use information about individuals. They must register the use of that information (through the Information Commissioner) and they must ensure that they follow sound practises in recording and using the information, in line with the Data Protection Principles.

3.3 The Data Protection Act 2018 covers all information that is held on computers or computer media, and any set of manual information relating to individuals to the extent that the set is structured, either by reference to individuals or by reference to criteria

relating to individuals, in such a way that specific information relating to a particular individual is readily accessible.

4. Definition of Terms

Personal Data - Data which relates to a living individual who can be identified from those data and other information which is, or is likely to come into the possession of the data controller, and includes any expression of opinion and any indication of the intention of the data controller, or any other person, in respect of the individual. Personal information that is held by the Town Council and subject to the provisions of the Data Protection Act includes information about employees, councillors and organisations, as well as suppliers of the Town Council.

Special Categories of Personal Data - Special category data is personal data which is more sensitive, and so needs more protection. Sensitive personal data - includes information about racial or ethnic origin, political opinions, and religious or other beliefs, trade union membership, medical information, sexual orientation, genetic and biometric data or information related to offences or alleged offences where it is used to uniquely identify an individual.

Data Controller - An individual or organisation who (either alone or jointly in common with other persons) determines the purposes for which and the manner in which any personal data is processed.

Data Subject - An individual who is the subject of personal data.

Data Protection Officer (DPO) - DPOs are normally appointed by organisations to assist in monitoring internal compliance, informing and advising on data protection obligations, and act as a contact point for data subjects and the supervisory authority. The GDPR states that organisations, including local councils and parish meetings will need to appoint a Data Protection Officer ("DPO") if they meet certain criteria. Local councils and parish meetings will not fall into the definition of a 'public authority' for the purposes of the Data Protection Act 2018. The rationale for this according to the debates in Parliament is that local councils and parish meetings will not normally be processing personal data 'on a large scale'. However larger local councils who do process personal data on a large scale may still have to appoint a DPO.

Information Commissioner - The Commissioner is an independent supervisory authority and has an international role as well as a national one. In the UK the Commissioner has a range of duties including the promotion of good information handling and the encouragement of codes of practice for data controllers, that is, anyone who decides how and why personal data, (information about identifiable, living individuals) are processed.

Disclosure - The passing of personal data to a third party, either an individual or an organisation

Data Protection Registration - The means of updating the official public register for the purposes of keeping personal data in the Council. It also includes descriptions of the data collected, the class of person the data relates to and to whom the personal data can be disclosed

Subject Access Request - The right of a data subject to have access to the information held about them. Data protection legislation mandates that Subject Access Requests are dealt with in the statutory timeframes of 1 month.

Third Party Any person other than - The data subject, The data controller or Any data processor or other person authorised to process data for the data controller or processor. The expression third party does not include employees or agents of the data controller.

Processing information or data - means obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data, including:

- organising, adapting or altering it
- retrieving, consulting or using the information or data
- disclosing the information or data by transmission, dissemination or otherwise making it available
- aligning, combining, blocking, erasing or destroying the information or data. regardless of the technology used.

5. Data Protection Principles

The following 6 principles must be applied to all processing of personal data:

5.1 The processing of personal data for any of the law enforcement purposes must be lawful and fair.

5.2 The law enforcement purpose for which personal data is collected on any occasion must be specified, explicit and legitimate. Personal data so collected must not be processed in a manner that is incompatible with the purpose for which it was collected.

5.3 Personal data processed for any of the law enforcement purposes must be adequate, relevant and not excessive in relation to the purpose for which it is processed.

5.4 Personal data processed for any of the law enforcement purposes must be accurate and, where necessary, kept up to date, and, every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the law enforcement purpose for which it is processed, is erased or rectified without delay.

5.5 Personal data processed for any of the law enforcement purposes must be kept for no longer than is necessary for the purpose for which it is processed.

5.6. Personal data processed for any of the law enforcement purposes must be so processed in a manner that ensures appropriate security of the personal data, using appropriate technical or organisational measures (and, in this principle, “appropriate security” includes protection against unauthorised or unlawful processing and against accidental loss, destruction or damage).

6. Individuals Rights

The UK GDPR provides rights for individuals in respect of personal data held about them by others, these are:

6.1 Right to Information

6.1.1 Individuals have the right to be informed about the collection and use of their personal data. This is a key transparency requirement under the UK GDPR.

6.1.2 The Council must provide individuals with information including: our purposes for processing personal data, our retention periods for that personal data, and who it will be shared with. We call this 'privacy information'.

6.2 Right to Access

6.2.1 All individuals have the right upon making a request in writing and providing the necessary identification documents, whether the individual or someone else on their behalf is processing personal data relating to that individual. If the individual is unable to make this request, they can do so through their authorised representative.

6.2.2 Individuals have the right to be given:

- A description of the personal data the Council holds
- The purposes for which it is being processed
- The categories of data being processed
- Those to whom it is, or may be, disclosed.

6.2.3 All requests must be dealt with promptly and within 1 month following receipt of a formal application.

6.3 Right to Rectification (correct inaccurate or incomplete data)

6.3.1 Individuals have the right to ask to rectify information that they think is inaccurate or incomplete. The Town Council has a duty to investigate any such claims and rectify the information where appropriate within 30 days, unless an extension of up to a further 60 days can be justified.

6.4 Right to be Forgotten (right to erasure)

6.4.1 The right for an individual to request that their data is erased is not absolute. It applies where:

- the information was given voluntarily, consent is now withdrawn and no other legal basis for retaining the information applies;
- the information is no longer required by the Town Council;
- a legal obligation to erase the data applies;
- the data was collected from a child for an online service;
- the Town Council has processed the data on the basis that it is in their legitimate business interests to do so, and having conducted a legitimate interests test, it concludes that the rights of the individual to have the data erased outweigh those of the Town Council to continue to process it.

6.5 Right to Restriction of Processing

6.5.1 An individual may ask the Town Council to temporarily limit the use of their data when it is considering:

- a challenge made to the accuracy of their data, or

- an objection to the use of their data.

6.6 Right to object

6.6.1 Individuals have a right to object in relation to the processing of data for

- for a task carried out in the public interest;
- for the exercise of official authority;
- for their legitimate interests;
- for scientific or historical research, or statistical purposes; or
- for direct marketing purposes.

6.6.2 Please note, if a data subject objects to direct marketing the Council cannot say no. However, if a data subject objects about other uses, the Council can refuse to comply with the objection.

6.7 Rights in Appropriate Decision Making (automated)

6.7.1 This does not apply as the Town Council does not employ automated decision making processes (i.e. making a decision solely by automated means without any human involvement and. profiling - automated processing of personal data to evaluate certain things about an individual).

6.8 Right to Data Portability

6.8.1 An individual can make a request in relation to data which is held electronically for it to be transferred to another organisation or to themselves where they have provided it either directly or through monitoring activities

6.8.2 This right is similar to your right of access but there are some differences. Specifically, the right only applies to data that:

- is held electronically, and
- the data subject has provided to the organisation.

6.8.3 A request can be verbal or in writing.

6.8.4 If the Council believes that a request is, as the law states, “manifestly unfounded or excessive”, it can:

- request a reasonable fee to deal with the request, or
- refuse to deal with the request.

6.8.5 In reaching this decision, we can take into account whether the request is repetitive. In either case the Council will inform the data subject and justify the decision.

7. Lawful Basis

7.1 How should we document our lawful basis?

7.1.1 The principle of accountability requires the Council to be able to demonstrate that we are complying with the UK GDPR, and have appropriate policies and processes. This means that we need to be able to show that we have properly considered which lawful basis applies to each processing purpose and can justify our decision.

7.1.2 We need therefore to keep a record of which basis we are relying on for each processing purpose, and a justification for why we believe it applies. There is no standard form for this, as long as we ensure that what we record is sufficient to demonstrate that a lawful basis applies.

7.2 What are the conditions for processing special category data?

7.2.1 If processing special category data, the Council need to identify both a lawful basis for processing and a special category condition for processing in compliance with Article 9. We document both the lawful basis for processing and the special category condition so that we can demonstrate compliance and accountability.

7.2.2 Article 9 lists the conditions for processing special category data:

(a) Explicit consent
(b) Employment, social security and social protection (if authorised by law)
(c) Vital interests
(d) Not-for-profit bodies
(e) Made public by the data subject
(f) Legal claims or judicial acts
(g) Reasons of substantial public interest (with a basis in law)
(h) Health or social care (with a basis in law)
(i) Public health (with a basis in law)
(j) Archiving, research and statistics (with a basis in law)

7.3 What are the substantial public interest conditions?

7.3.1 The 23 substantial public interest conditions are set out in paragraphs 6 to 28 of Schedule 1 of the DPA 2018:

6. Statutory and government purposes
7. Administration of justice and parliamentary purposes
8. Equality of opportunity or treatment
9. Racial and ethnic diversity at senior levels
10. Preventing or detecting unlawful acts
11. Protecting the public
12. Regulatory requirements
13. Journalism, academia, art and literature
14. Preventing fraud
15. Suspicion of terrorist financing or money laundering
16. Support for individuals with a particular disability or medical condition
17. Counselling
18. Safeguarding of children and individuals at risk

19. Safeguarding of economic well-being of certain individuals
20. Insurance
21. Occupational pensions
22. Political parties
23. Elected representatives responding to requests
24. Disclosure to elected representatives
25. Informing elected representatives about prisoners
26. Publication of legal judgments
27. Anti-doping in sport
28. Standards of behaviour in sport

8. Handling of Personal/Sensitive Information

8.1 In compliance with the Act, the Town Council will:

- Ensure that personal data is obtained fairly and lawfully
- Acknowledge the rights of individuals relating to personal data and ensure that these rights can be exercised as specified in the Act
- Meet its legal obligations to specify the purpose for which information is used
- Inform data subjects of data processing activities with a published fair processing notice (The notice explains how personal data will be 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
- Take appropriate measures to safeguard personal information

9. Implementation

9.1 The Clerk to Yarm Town Council is responsible for ensuring adherence with the Data Protection Act.

10. Notification to the Information Commissioner

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

10.2 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.

10.3 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.

10.4 The Town Council is registered as a Data Controller with the ICO. Our reference number is Z263793X.

11. Scope of this Policy

11.1 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.

11.2 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.

11.3 Emails will be purged regularly and deleted safely.

11.4 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.

12. Responsibilities

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

12.2 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.

12.3 Yarm 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.

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

13. Data Received and Created by Town Councillors

13.1 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 1998/2018 and Freedom of Information Act 2000.

13.2 It is recognised that members of the public may contact Yarm 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.

13.3 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.

13.4 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.

13.5 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.

14. Retention of Documents or Electronic Data

14.1 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.

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

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

15. Disclosure of Personal Information

15.1 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 overhanging bushes from a YTC park into 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.

16. Other Documents Including Written Notes of the Clerk and Councillors

16.1 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.

16.2 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.

17. Documentation Relating to Staff/Personal Information

17.1 Staff/personal information should be kept securely and in accordance with the Eight Data Protection Principles contained in the Data Protection Act 1998/2018. 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.