



GREAT TORRINGTON TOWN COUNCIL

GENERAL DATA PROTECTION REGULATION POLICY

May 2023

CONTENTS

1. Purpose of the policy and background to the General Data Protection Regulation (GDPR)
2. The Scope of this Policy
3. Identifying the roles and minimising risk
4. Data Protection Principles
5. The Lawful bases of processing
6. Data breaches
7. Privacy Notices
8. Information Audit
9. Individuals' Rights
10. The two enhancements of GDPR
11. Children
12. Summary
13. Document Record

1. Purpose of the policy and background to the General Data Protection Regulation (GDPR)

This policy explains to councillors, staff, role holders and the public about GDPR. Personal data must be processed lawfully, fairly and transparently; collected for specified, explicit and legitimate purposes; be adequate, relevant and limited to what is necessary for processing; be accurate and kept up to date; be kept only for as long as is necessary for processing and be processed in a manner that ensures its security. This policy includes the additional requirements of GDPR which apply in the UK from May 2018. This policy explains the duties and responsibilities of the Town Council and it identifies the means by which the council will meet its obligations.

2. Scope of the Policy

This policy applies to all data created, received or maintained by the Town Council in the course of carrying out its functions. Data

Data is defined as all personal data of anyone involved in the business carried out by the Town Council.

3. Identifying the roles and minimising risk

GDPR requires that everyone within the Council must understand the implications of GDPR and that roles and duties can be assigned.

- A Data Subject is an individual who is the subject of personal data;
- The Council is the Data Controller;
- The Town Clerk is the Data Protection Responsible Officer (DPRO).

It is the DPRO's duty to undertake an information audit and to manage the information collected by the Council, the issuing of privacy statements, dealing with requests and complaints raised and also the safe disposal of information.

- The Data Processor is the person who processes data on behalf of the Data Controller.

GDPR requires continued care by everyone within the Council, councillors and staff, in the sharing of information about individuals, whether as a hard copy or electronically. A breach of the regulations could result in the Council facing a fine from

the Information Commissioner's Office (ICO) for the breach itself and also to compensate the individual(s) who could be adversely affected. Therefore, the handling of information is seen as medium risk to the Council (both financially and reputational). Such risk can be minimised by undertaking an information audit, issuing privacy statements, maintaining privacy impact assessments (an audit of potential data protection risks with new projects), minimising who holds data protected information and the Council undertaking training in data protection awareness.

4. Data Protection Principles

It is the duty of a data controller to comply with data protection principles. These are summarised in that personal data;

- Must be processed fairly and lawfully and in a transparent manner;
- Must be collected and held only for specified, explicit and lawful purposes;
- Must be adequate, relevant and limited to what is necessary for the purposes for which it is processed;
- Must be accurate and kept up-to-date;
- Must not be kept for any longer than is necessary for the stated purpose;
- Must be processed in a manner that ensures appropriate security of the personal data;
- Must have appropriate technical and organizational safeguards against unauthorised or unlawful processing; must not be transferred to any country outside of the European Economic Area unless that country has an adequate level of protection of the rights and freedoms of the data subjects.

5. Lawful bases of Processing

- Consent
- Contract

- Legal Obligation
- Vital Interests
- Public Tasks

6. Data breaches

One of the duties assigned to the DPRO is the investigation of any breaches. Personal data breaches should be reported to the DPRO for investigation. The DPRO will conduct this with the support of the Town Council. Investigations must be undertaken within one month of the report of a breach. The ICO will be advised of a breach (within 3 days) where it is likely to result in a risk to the rights and freedoms of individuals – if, for example, it could result in discrimination, damage to reputation, financial loss, loss of confidentiality, or any other significant economic or social disadvantage. Where a breach is likely to result in a high risk to the rights and freedoms of individuals, the DPRO will also have to notify those concerned directly.

It is unacceptable for non-authorised users to access IT using employees' log-in passwords or to use equipment while logged on. It is unacceptable for employees, volunteers and members to use IT in any way that may cause problems for the Council, for example the discussion of internal council matters on social media sites could result in reputational damage for the Council and to individuals.

7. Privacy Notices

Being transparent and providing accessible information to individuals about how the Council uses personal data is a key element of the Data Protection Act 1998 (DPA) and the EU General Data Protection Regulation (GDPR). The most common way to provide this information is in a privacy notice. This is a notice to inform individuals about what a Council does with their personal information. A privacy notice will contain the name and contact details of the data controller and Data Protection Officer, the purpose for which the information is to be used and the length of time for its use. It should be written clearly and should advise the individual that they can, at any time, withdraw their agreement for the use of this information. Issuing of a privacy notice must be detailed on the Information Audit kept by the Council. The Council will adopt a privacy notice to use, although some changes could be needed depending on the situation, for example where children are involved.

8. Information Audit

The DPRO must undertake an information audit which details the personal data held, where it came from, the purpose for holding that information and with whom the Council will share that information. This will include information held electronically or as a hard copy. Information held could change from year to year with different activities, and so the information audit will be reviewed at least annually or when the Council undertakes a new activity. The information audit review should be conducted ahead of the review of this policy and the reviews should be minuted.

9. Individuals' Rights

GDPR gives individuals rights with some enhancements to those rights already in place:

- the right to be informed
- the right of access
- the right to rectification
- the right to erasure
- the right to restrict processing
- right to data portability
- the right to object
- the right not to be subject to automated decision-making including profiling.

10. The two enhancements of GDPR are;

- That individuals now have a right to have their personal data erased (sometime known as the 'right to be forgotten') where their personal data is no longer necessary in relation to the purpose for which it was originally collected and data portability must be done free of charge.
- Data portability refers to the ability to move copy or transfer data easily between different computers.

If a request is received to delete information, then the DPRO must respond to this request within a month. The DPRO has the delegated authority from the Council to delete information.

If a request is considered to be manifestly unfounded then the request could be refused or a charge may apply. Council will be informed of such requests.

11. Children

There is special protection for the personal data of a child. The age when a child can give their own consent is 13. If the Council requires consent from young people under 13, the Council must obtain a parent or guardian's consent in order to process the personal data lawfully. Consent forms for children age 13 plus, must be written in language that they will understand.

12. Summary

In summary, the main matters arising within this policy are:

- The Council must be registered with the ICO.
- A copy of this policy will be available on the Council's website. The policy will be considered as a core policy for the Council.
- The Clerk's Contract and Job Description (if appointed as DPRO) will be amended to include additional responsibilities relating to data protection.
- An information audit will be conducted and reviewed at least annually or when projects and services change.
- Privacy notices must be issued.
- The Town Council will manage the process.

This policy document is written with current information and advice. It will be reviewed at least annually or when further advice is issued by the ICO.

All employees, role holders and councillors are expected to comply with this policy at all times to protect privacy, confidentiality and the interests of the Council.

13. Document Record

Document	General Data Protection Policy
Lead Author(s):	Karen Chapman – Town Clerk
Developed by:	Great Torrington Town Council
Approved by/Date	Policy and Finance 23.09.20
Ratified/Adopted and date:	Council Meeting 01.10.20
Review Date:	August 2022
Version:	2