TORBAY COUNCIL

Data Protection Policy

2020

Contents

This document can be made available in other languages and formats.

For more information please contact infocompliance@torbay.gov.uk

Document Control	
Organisation	Torbay Council
Creator	Head of Information Governance & DPO
Approvals	Information Governance Steering Group
Distribution	Public and Corporate
Review	2 years

Document Amendment History

Version Number	Originator	Date of Change	Change description
1.1	Jo Beer	May 2018	Policy Creation
1.2	Jo Beer	Sep 2020	Policy review and update

1. Introduction

This policy formalises Torbay Council's (the Council) approach to data protection legislation and how we will comply with the General Data Protection Regulation (GDPR) and Data Protection Act 2018.

In order for us to provide effective and efficient services we need to hold and process information about our customers. It is our responsibility to ensure that any information which is collected, held and shared is done so in accordance with data protection law.

For the majority of the information we hold and process Torbay Council is the 'data controller' under the GDPR. As a controller we determine the purpose and means of processing personal data However, there are instances where we also process personal data on behalf of other organisations and in these instances Torbay Council is considered to be a 'data processor'.

This policy applies to any information which we process about individuals which either identifies them or makes them identifiable, it applies to paper records as well as electronic records.

2. Roles and Responsibilities

Chief Executive and Senior Leadership Team

The Chief Executive and the Senior Leadership Team have ultimate responsibility for ensuring all departments across the Council comply with data protection law, they are also accountable for our compliance and must ensure an effective Council-wide information management approach.

Caldicott Guardian

The Caldicott Guardian is a senior officer responsible for protecting the confidentiality of information about our customers as well as enabling appropriate information sharing specifically in relation to information processed by social care services.

Senior Information Risk Owner (SIRO)

The SIRO has ownership of the risks associated with the information assets we hold and should act as an advocate for the organisation's information risk.

Data Protection Officer (DPO)

This is a mandatory requirement for all public authorities, therefore we must have in place a Data Protection Officer who is responsible for monitoring our compliance to data protection law and advising the senior leadership team and all staff of their roles and responsibilities. The role of the DPO is outlined further under section eight of this policy.

Information Governance Team

The Information Governance Team supports the Data Protection Officer in ensuring that the Council complies with data protection law. They support the whole Council in ensuring that requests made for information under data protection legislation are carried out in accordance with the legislation and local policies.

3. How the Council will comply with the principles of GDPR

The GDPR sets out six principles that all organisations must adhere to. The Council is responsible for, and must be able to demonstrate, compliance to these principles. The principles are as follows.

Personal data shall be:

- Processed lawfully, fairly and in a transparent manner.
- Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

- Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).
- 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 (accuracy).
- 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 in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject (storage limitation / retention).
- 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 (‘integrity and confidentiality’).

3.1 Personal data shall be processed lawfully, fairly and in a transparent manner

We will only hold and process personal data where we have a lawful basis to do so. For most of the services we provide, we will need to hold personal data because it is necessary to fulfil a task which hawse have an official authority to carry out, for example, the we have a duty to collect Council Tax and cannot do so without knowing who is liable for the tax at a property. Therefore information will be held about who is liable along with bank details for the purpose of direct debit payments.

Where we are relying on consent to process your information, t we will ensure that you have a clear opt in for the processing and that you have the option to withdraw your consent at any time. We shall be clear about what you are consenting to and shall keep a record which demonstrates this consent has been provided.

In order to process personal data fairly and transparently, you will be informed as to what is being done with your personal data by way of a Privacy Notice. All of our privacy notices will set out the following:

- The purpose for which personal data will be processed
- The lawful basis the Council is relying on to process the personal data
- How long the personal data shall be kept for
- Who and which organisations the personal data might be shared with and for what purpose
- Whether the personal data is subject to any international transfers
- The rights which you can exercise in relation to your own personal data and how you can exercise these rights

- How you can raise a complaint with the Council or with the Information Commissioner's Office.

We will always aim to provide you with this privacy notice at the point at which the personal data is collected. Where this is not possible; the privacy notice will be provided at the earliest opportunity. For example, where a referral is made to our Children's Services department, we will, from that point, be holding information about the family who are subject to the referral, at this point the family may not know the referral has been made. In this case a privacy notice would be issued to the family on initial contact.

Privacy notices will not be provided where an individual has already received a copy, where it would involve disproportionate effort to do, or where we do not need to provide a copy because an exemption exists, for example, for the prevention and detection of crime.

3.2 Specified, explicit and legitimate purpose and not processed in a manner incompatible with those purposes.

Information will only be used for the purpose for which it was originally collected. If it is necessary to use the information we hold in a new or different way, we will make contact with you and explain the proposed additional use of the information.

3.3 Adequate, relevant and limited to what is necessary (data minimisation)

We will only hold the minimum amount of personal data necessary in order to ensure the effective delivery of services provided.

We will make sure that:

- Information processed will be limited to what is necessary for the purpose and no more information will be collected than is required. For example, we will not ask for a date of birth if knowing an age-range is sufficient for the purpose.
- Information will not be held for longer than is necessary for the original purpose or be kept past its retention period (the point after which information must be deleted).

3.4 Accurate and where necessary kept up to date (accuracy)

The accuracy of the information which we hold is important in ensuring the effective provision of service. If you believe that information we hold about you is inaccurate you can request, under the right to rectification, that inaccurate information is changed. However, in a situation where a professional has recorded their opinion, we will expect that professional opinion is stated as such. As opinions are not a statements of fact, we will not consider any challenge in respect of their accuracy.

Where individuals have notified us of any change in their circumstances, or have a valid request made under the right to rectification, we will update and comply with the request in a timely manner and in accordance with our Information Rights Policy.

3.5 Kept in a form which permits identification for no longer than necessary (retention)

We process a wide range of information for the many different services we provide. Each different type of processing activity, or information asset will have its own associated retention period (time after which the information must be deleted). We hold a Records Retention Schedule and this is based on professional guidelines or legal requirements. It is the responsibility of each department to ensure that they delete data in accordance with their retention periods and that all personal data is destroyed securely.

3.6 Processed in a manner which ensures appropriate security (integrity and confidentiality)

We will ensure that appropriate security measures are put in place to protect the integrity, confidentiality and availability of the information being processed. This includes protecting personal information from the following:

- Unauthorised access or disclosure
- Accidental or unlawful destruction, loss or alteration

In order to comply with this principle we will assess the processing activities and assess the risk to the rights and freedoms of our customers. In response to these assessments we will put in place technical and organisational measures which are appropriate and proportionate to the risk of the personal data being processed.

Technical measures may include ensuring appropriate password controls on IT systems and databases, ensuring that paper records are stored in locked cabinets, and that mobile devices have appropriate encryption to protect information in the event of loss or theft.

Organisational measures have been put in place in order to ensure that staff are aware of their responsibilities under data protection law. All staff members are appropriately trained to use our secure IT systems and this is reflected in policies outlining expectations for safe and secure data handling.

3.7 Rights of individuals

The GDPR sets out a number of rights which you can exercise in relation to how your personal data is processed by organisations. We have a separate Information Rights Policy which covers

the handling of requests made under these rights. This policy can be found at www.torbay.gov.uk/council/information-and-data

3.8 International Transfers

We will not transfer any personal data outside of the European Economic Area (EEA), without first ensuring that there are adequate safeguards in place to ensure the security of the personal data being transferred. This includes, the storage of any personal data on servers, including hosted systems which we may purchase and officers taking mobile devices, such as iPads, laptops, mobile phones abroad with them. Any transfer of personal data outside of the EEA will be subject to a risk assessment and must be approved by our Data Protection Officer and the SIRO.

4. Special categories of personal data

We will often have to process information about individuals which, under the GDPR, is considered to be 'special category' data, this will consist of the following:

- Data revealing a person's race or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade Union membership
- Genetic data or biometric data for the purpose of uniquely identifying an individual
- Data concerning a person's health
- Data concerning a person's sex life or sexual orientation

We will not process special category data unless we are able to demonstrate that a second lawful basis applies. We will also ensure that additional safeguards are put in place to protect any personal data fall under these categories and will be clear with individuals about when and why this type of information shall be processed.

5. Processing of personal data for law enforcement

We do, under some circumstances, process personal data for 'law enforcement purposes'. This is because we have statutory duties which relate to the prevention, investigation, detection or prosecution of criminal offences. Part 3 of the Data Protection Act 2018, sets out what we must do with the personal data we process for law enforcement purposes. Therefore, as we have statutory law enforcement duties, we will comply with the requirements set out in Part 3 of the Act 2018.

6. Records of Processing Activities

Under the GDPR, we are required to keep 'records of processing activities'. These records should set out what personal data we are processing and why. We will do this through our Information Asset Register. This register will hold details of the different types of information that we process. It will also record: the purpose for which we hold the information, the lawful basis alongside the associated retention periods, the number of records held and the officers responsible for the asset (Information Asset Owners). The Information Asset Owners are members of our Senior Leadership to ensure accountability for the processing activities of services. These records will be maintained by Information Asset Administrators within each service and will be subject to regular review by our Data Protection Officer and internal audit department.

7. Data Protection Impact Assessments (DPIA)

Under the GDPR it is a requirement to carry out a DPIA where we will be using new technologies and / or where new processing activities will be carried out on personal data, where it is considered that this could result in a high risk to the rights and freedoms of individuals. This assessment will allow services to demonstrate how their processing activities will comply with data protection legislation, but also to outline any potential risks to the rights and freedoms of individuals, ensuring that appropriate mitigations can be put in place to minimise these risks.

The advice of our Data Protection Officer must be sought when carrying out a DPIA. The DPIA must be approved by our Data Protection Officer and our SIRO before a system is purchased or the processing activity begins.

DPIAs must be regularly reviewed to ensure that the risks to the personal data continue to be appropriately mitigated.

7. Data Processors

There may be times when we engage other organisations to carry out a task on our behalf which could include the processing of personal data. In these situations we will always check the organisation's compliance to data protection legislation and their information security policies and procedures. Before any processing is carried out on our behalf a contract must be agreed between both parties. This Data Processing Agreement will set out what processing activity is to be carried, the duration of the processing contract, the type of personal data and categories of data subject, as well the rights and obligations of the Council.

8. Data Protection Officer (DPO)

As a public authority we are required to have a DPO. At Torbay Council this role is designated to the Head of Information Governance. This post reports directly to the Council's Senior Leadership Team through the Assistant Director for Corporate Services.

We are is committed to ensuring that the DPO is able to independently undertake the tasks set out within the GDPR and shall be provided with any support which may be required.

The DPO will:

- Inform and advise our Senior Leadership Team and our officers of their responsibilities under data protection legislation.
- Monito our compliance to data protection legislation and our own policies in relation to data protection, information rights, information governance and security and records management.
- Raise awareness and provide training to staff involved in processing personal data.
- Provide advice on DPIAs.
- Have due regard to the risks associated with data processing activities.
- Investigate any breaches of personal data and make recommendations for action / improvement.
- Act as a point of contact for members of the public in relation to any issues regarding the processing of their personal data, in regards to the exercising of their rights.
- Cooperate with the Information Commissioner's Office and act as the single point of contact on issues relating data processing.

We will publish the contact details for the DPO.

9. Handling breaches of personal data

Where any breaches of personal data occur all staff across the Council have a responsibility to notify the Data Protection Officer as soon as they become aware of the breach, even if they are unsure whether a breach has actually occurred. A breach of personal data is defined as:

> 'A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised access to; personal data transmitted, stored or otherwise processed.'

We recognise that if a personal data breach is not addressed appropriately and promptly, then the risks to the rights and freedoms of those individuals who may be affected can increase. Therefore we are committed to ensuring that personal data breaches will always be investigated promptly,

with any immediate actions required being undertaken to recover the personal data where possible.

Where it is determined that the breach could result in a high risk to the rights and freedoms of those affected, we will notify the Information Commissioner's Office (ICO) within 72 hours of becoming aware of the breach and, where appropriate and possible, will notify the individuals affected.

To determine whether a breach could result in a high risk to the rights and freedoms of those affected, we will assess how many people are affected, the information subject to the breach and the potential impact on those individuals.

We also require that any data processors acting on our behalf must report any personal data breaches within 24hours to ensure that we can comply with the requirements to report any breach to the ICO.

In undertaking an investigation the Data Protection Officer, or a member of the Information Governance Team, will consider the technical and organisational measures which were in place to protect the personal data. Associated policies will be analysed to determine if any improvements need to be made and any recommended actions will be issued to the service area responsible for the breach.

Should a member of staff cause (or potentially have caused) a personal data breach and does not notify the Data Protection Officer, this will be considered a disciplinary issue.

10. Monitoring and review

This policy and those policies which sit underneath this framework will be reviewed every two years and updated accordingly.