Data Protection Policy

May 2018

Version Control Sheet

Title	Data Protection Policy (incorporating requirements of European General Data Protection Regulations 2018 and UK Data Protection Act 2018)
Author	Judy Barker Information Governance & IT Services Manager Tendring District Council
Approved by	Information Governance Policy Unit
Date	11 April 2017
Version Number	1
Status	DRAFT
Review Frequency	Annual or following any amendment to relevant Information and Governance Legislation
Next Review Date	October 2019

Amendment History / Change Record

Date	Version	Key Changes / Sections Amended	Amended By
May 2018	1	Updated to include DPA 2018 and final published textual requirements	Judy Barker

Contents **Page**

1. Introduction

This is a statement of the Data Protection Policy adopted by Tendring District Council.

The Council needs to collect and process personal information about individuals so that it can operate and provide services. Personal Data includes information relating to current, past and present employees, elected members, suppliers, residents and other members of the public with whom it communicates. The Council is also required by law to collect and use some types of information to comply with the rules of government departments.

The Data Protection Act 2018 (incorporating the European General Data Protection Regulation (**GDPR**))**,** replaced the previous Data Protection Act 1998 **(DPA)** on **25 May 2018** but ***continues*** to serve the purpose **of protecting the privacy rights of living individuals**. The Act requires the secure and lawful collection, processing, sharing and disposal of personal information whether on paper (including handwritten notes), in electronic form, or recorded on other material such as CCTV images and voice recordings.

As the GDPR is a Regulation, it will not be separately interpreted into the domestic laws of each member state. However, each member state's activities will be controlled by a supervisory authority within the country where the greatest percentage of the processing takes place. This will continue to be the UK Information Commissioner's Office (ICO) for Great Britain and is incorporated into the Data Protection Act 2018.

2. Policy Statement and Scope

The Council is required by law to protect the public funds it administers. In order to meet this obligation this will include sharing information internally and externally to prevent and detect fraud, improve the way it delivers services and for the purpose of performing any of its statutory enforcement duties. This will also include sharing information with other bodies responsible for auditing and administering public funds. All personal information will be processed in accordance with the provisions of the Data Protection Act.

The Act requires the Council to collect, process, share and dispose of personal information securely and correctly. This Council recognises that the lawful and correct treatment of personal information is essential to the delivery of successful operations to our customers and maintaining the confidence of the individuals to whom the data relates (internally and externally).

The Council requires all of its employees, elected members and third parties operating on our behalf to comply with this policy and to cooperate with all measures and procedures in place to ensure legal compliance.

To this end, this organisation fully endorses and adheres to the principles of data protection.

3. The Principles

The Principles relate to the processing of personal data stating that it shall be:-

- Processed lawfully, fairly and **in a transparent manner** in relation to the data subject ('lawfulness, fairness and transparency'); **(Principle 1)**
- 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 purpose or statistical purposes, shall not be considered to be incompatible with the initial purpose); **(Principle 2)**
- Adequate, relevant and limited to **what is necessary** in relation to the purposes for which they are processed ('data minimisation'); **(Principle 3)**
- 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') **(Principle 4)**
- 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 as long as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical or statistical research purposes, as long as they are subject to implementation of the appropriate technical and organisational measures (e.g. anonymisation) required to safeguard the rights and freedoms of the data subject under this legislation ('storage limitation'); **(Principles 5 & 6).**
- 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') **(Principle 7)**

Note: **GDPR** compliance is required by every organisation that offers goods and services to people in the European Union (EU), or that collect and analyses data tied to EU residents The GDPR applies no matter where the organisation (the controller) is located. The UK Data Protection Act exists to protect the privacy rights of UK citizens.

4. Data Protection Officer

4.1. Requirement & Role

The law requires all public authorities to designate a Data Protection Officer. A summary of the responsibilities of this role are to:-

- Inform and advise the controller (the Council), and its employees who carry out processing, of their obligations;
- Monitor compliance, with the Act and policies of the controller in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- Provide advice where requested as regards the data protection impact assessment and monitor its performance;
- Cooperate with the supervisory authority (UK Information Commissioner); and

- Act as the contact point for all issues relating to the processing of personal information.

4.2. Contact details

The contact details of the council's Data Protection Officer are published in the Privacy Notice.

4.3. Training and Awareness

The Council has an obligation to ensure its staff are trained in their obligations and responsibilities in the handling and security of personal information. The council has a mandated data protection awareness programme in place to deliver this requirement.

5. Security and Information We Hold

5.1. Privacy Notice

The Council's privacy notice is published on the council's website. A paper copy is also held at each public reception area. A link to the privacy notice is included in the automatic footer which is added to all external emails.

In addition to this the council will ensure it has a process in place to ensure fair processing of information is always carried out at the point personal information is collected from individuals. The council's privacy notice will:-

- Include details regarding the organisation and contact information for the Council's Data Protection Officer;
- Be accessible, transparent and written in plain English so that they are easily understood;
- Contain sufficient detail so that it is clear to individuals that the collection, processing and purpose of personal data concerning them is explicit and legitimate;
- Include details of the rights of individuals and how they can exercise those rights;
- Confirm that data will only be kept for as long as necessary (i.e. in accordance with statutory timeframes and the Council's information retention policy);
- Provide an undertaking that every reasonable step will be taken to ensure that inaccurate personal data will be rectified or deleted.

5.2. Security and Privacy Impact Risk Assessment

The council will undertake a Data Protection Impact Assessment when:

- Using new technologies
- The processing is likely to result in a high risk to the rights and freedoms of individuals

6. Rights of Individuals

6.1. Summary of Rights

- The right to be informed
- The right of access (see Section 6.2 below)
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights related to automated decision making and profiling

6.2. Requests for disclosure of Personal Information (Right of Access)

All individuals have a right of access to their own personal information. Any request by an individual for access to their own information must be considered a Right of Access request under this legislation. Normal, day to day transaction type enquiries will continue to be handled by the relevant business area; but all other requests for personal information will be managed centrally by the Data Protection Officer to ensure that statutory deadlines are achieved. An example of when this would apply is shown below.

Example :- a housing tenant requests the outstanding balance on their account – this would be a normal business transaction. If the same tenant asks for a copy of all the records associated with their tenancy, including emails and file notes, plus copies of everything that Revenues and Benefits hold, then this will be managed centrally by the Data Protection Officer.

7. Legal Basis for Processing Personal Data

7.1. Lawful Processing

The Council will only process personal data if **at least one** of the following applies:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party, or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation (UK Law) to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (under UK Law);

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller (the Council) or by a third party, except where such interests are

overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. However, this point (f) shall not apply to processing carried out by public authorities in the performance of their tasks (see Statutory Obligations)

Please note that, where the processing of data is for a purpose other than that for which it was collected and the data subject's consent has not been obtained, the Council is required to consider the following to ensure that the proposed additional processing purpose is compatible with the purpose for which it was initially collected. The outcome of this consideration will be documented along with the reasons why. This file note will be retained as evidence of the decision.

- Any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
- The context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
- The nature of the personal data, in particular whether special categories (formally referred to Sensitive Personal Data) of personal data are processed or whether personal data related to criminal convictions and offences are processed and the possible consequences of the intended further processing for the data subjects themselves;
- The existence of appropriate safeguards, which may include encryption or pseudonymisation.

7.2. Statutory Obligations

Local authorities are bound by statute and their functions and obligations are set out in numerous Acts of Parliament, many of which have associated legal duties.

Any and all processing of personal data in order to carry out any statutory obligation will be undertaken in compliance with the requirements of the relevant legislation governing the statutory obligation and the principles of the data protection.

7.3. Information Sharing Protocols

Where a decision has been made to engage with the regular and/or systematic sharing of personal data, an Information Sharing Protocol and associated agreement will be specified for each sharing purpose. A privacy impact assessment may be required to identify and mitigate the risks involved.

7.4. Consent

Where the processing of personal information is not carried out to comply with a statutory or legal obligation, then consent may need to be obtained from the data subject involved.

The consent must be a freely given, specific, informed and unambiguous statement of the data subjects agreement to the processing. Consent will not be assumed to be provided by silence or a non-response to a request.

The consent will be recorded in writing or by electronic means. If a verbal consent statement is unavoidable it will be recorded and witnessed for future review.

In order to be 'freely given' it is important to seek consent only where the processing is optional, as consent can also be withdrawn at any time.

7.5. Processing of Children's Data

Specific protection of the personal data relating to children is essential as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.

Such specific protection will particularly apply to the use of personal data for the purposes of marketing or creating personality or user profiles; for example in the collection and processing of personal data for use in relation to services being offered directly to a child (e.g. leisure), and parental consent will be sought where it is appropriate to do so, based on the service and/or the age of the child.

The consent of the holder of parental responsibility should not be necessary in the context of preventive or counselling services offered directly to a child.

7.6. Retention of Information

Data Protection legislation does not provide specific retention periods for personal data. However, in order to comply with the Principles, data must only be retained for as long as is necessary to fulfil the purpose for which it was collected. Statutory obligations to retain data for longer will be complied with.

The Council's Corporate Retention Policy and associated Schedule will provide guidance in this regard.

8. International transfers

Where regular transfers of personal data are required outside of the UK, suitable international transfer agreements will be set up to include the use of binding corporate rules. Measures will be put in place to protect all essential principles and enforceable rights to ensure appropriate safeguards for transfers or categories of transfers of personal data.

9. Breaches and/or Complaints

If any potential breach of data protection is suspected or identified, the Information Security Incident Response Procedure will be followed. This process will ensure a rapid response by the appropriate resources within the Council to look into the incident.

Any complaint received regarding the Council's handling of personal data should be directed to the Data Protection Officer.