Thurrock Council
Data Protection Policy

Information Management team

Version control

Title	Data Protection Policy
Purpose	To outline the requirements for the council to comply with the Data Protection Act 2018
Author	Strategic Lead – Information Management
Approved by	People Board
Date	25 February 2021
Version number	2.0
Status	Final
Review frequency	Every 3 years or at the point there are changes to information governance legislation
Next review date	25 February 2024

Amendment history / change record

Date	Version	Key changes / sections amended	Amended by
February 2021	2.0	Key changes: • mandated training frequency details added into 4.3 • added section 10 to the policy (ROPA) • added section 11 to the policy regarding Data minimisation	Strategic Lead – Information Management

Contents

1. Introduction

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 Data Protection Act 2018 (DPA) and General Data Protection Regulation (GDPR) replaced the previous Data Protection Act 1998 on 25 May 2018 but continues to serve the purpose of protecting the privacy rights of living individuals. The new Act and Regulation (now UK GDPR) 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.

2. Policy statement and scope

The council is required by law to protect the public funds it administers. In order to meet this obligation it 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 DPA.

The DPA requires the council to collect, process, share and dispose of personal information securely and correctly. The 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')
- 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 inaccurate personal data is erased or rectified without delay
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed
- 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')

4. Data Protection Officer

4.1. Requirement and role

Under the DPA all public authorities are required to designate a Data Protection Officer. In summary, the Data Protection Officer has responsibilities to:

- inform and advise the controller (the council), and its employees who carry out processing, of their obligations pursuant to this Regulation
- monitor compliance with this Regulation and with the 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 with regards to data protection impact assessment and monitor its overall performance
- co-operate with the supervisory authority (Information Commissioner)
- 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:

Lee Henley,
Strategic Lead – Information Management,
Thurrock Council,
Civic Offices,
New Road,
Grays.
RM17 6SL

Email – lhenley@thurrock.gov.uk

4.3. Training and awareness

The council has an obligation to ensure its staff (including Members) are trained in their duties and responsibilities in the handling and security of personal information. The council has a mandated data protection programme in place to deliver this requirement whereby:

- all new staff/members will undertake data protection training at the point of joining the council
- all existing staff/members will be required to undertake data protection refresher training approximately every 18 months
- different levels of training are available subject to the role of the member of staff

5. Security and information we hold

5.1. Privacy notice(s)

The council's privacy notice is available on our website. In addition to this the council will have 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 notices 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 – that is, in accordance with statutory timeframes and the council's information retention policy

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 DPA includes a number of rights for individuals. These are summarised as:

- 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

Further information can be found in the Individuals' Rights document, which is available on the council's website.

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. Additional information on the Right of Access is available on the council's website.

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 (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

Point (f) shall not apply to processing carried out by public authorities in the performance of their tasks (see Statutory Obligations). However, legitimate interests could apply if the council can demonstrate that the nature of the processing is not part of its role in performing tasks as a public authority – for example, fundraising.

7.2. Processing of special categories of data

Special categories of personal data under DPA are:

- racial or ethnic origin
- political opinions
- religious or philosophical beliefs
- trade union membership
- genetic data
- biometric data for the purpose of uniquely identifying a natural person
- health data
- sex life or sexual orientation

For the council to process any of the above special categories of data, it must ensure that it can meet at least one of the conditions detailed in (a) to (j) below, in addition to at least one condition in 7.1:

(a) the Data Subject have given explicit consent to the processing

(b) to carry out tasks under employment, social security or social collective law

(c) to protect the vital interests of a person who is physically or legally unable to give consent

(d) processing carried out by a not-for-profit body with a political, philosophical, religious or trade union aim provided the processing relates only to members or former members (or those who have regular contact with it in connection with those purposes) and provided there is no disclosure to a third party without consent

(e) if the data has already been made public by the individual

(f) to establish, exercise or defend a legal claim

(g) processing is necessary for reasons of substantial public interest

(h) processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional

(i) to protect the public interest in public health

(j) to enable archiving of data that has a public interest – that is, scientific, historical research or for statistical purposes

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 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, and this file note will be retained as evidence of the decision:

- any link between the purposes for which the personal data has been collected and the purposes of the intended further processing
- the context in which the personal data has 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 as 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

7.3. 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 DPA.

7.4. 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.

7.5. Consent

If consent is relied upon to process personal data, then this 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.

7.6. 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 (for example, 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.

7.7. Retention of information

The DPA 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 the DPA is suspected or identified, the Information Security Incident Response Procedure will be followed. This process will ensure a rapid response by 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 (contact details in 4.2 above).

10. Record of Processing Activity (ROPA)

The council has identified its data processing activities by mapping out its key information assets on a central Record of Processing Activity (ROPA). A corporate information governance group has been set up to maintain the ROPA.

11. Data minimisation

The council will identify and collect the minimum amount of personal data it needs to fulfil its purposes. This will be verified by undertaking checks as part of the work of the Information Governance Group.