

Data Protection Policy

Information Governanace

26/09/2022



Table of Contents

1.0 Introduction and Scope	4
2.0 Data Protection Principles	4
2.1 Lawfulness, fairness, and transparency.....	5
2.2 Purpose Limitation	5
2.3 Data Minimisation	5
2.4 Accuracy.....	5
2.5 Storage Limitation and Data Retention	6
2.6 Integrity and Confidentiality	6
2.7 Accountability.....	6
3.0 Roles and Responsibilities	7
3.1 Chief Executive.....	7
3.2 Senior Information Risk Owner (SIRO).....	7
3.3 Information Asset Owner (IAO).....	7
3.4 Head of Information Security	7
3.5 Head of Information Governance.....	7
3.6 Data Protection Officer	7
3.7 All Managers.....	7
3.8 All Staff, Contractors, and Authorised Third Parties.....	7
4.0 Data Subject Rights.....	8
5.0 Data Protection by design and default.....	9
6.0 Personal Data Incidents and Breaches	9
7.0 Key Controls.....	10
8.0 Compliance Monitoring.....	11
9.0 Training	11
10.0 Who to contact for further help	11
11.0 Definitions	11
12.0 Policy Review.....	12
13.0 Policy Signoff.....	12

Data Protection Policy

Version	Date	Amendment Details	Version	Author
7.0	July 2022	Significantly updated from v.6 (approved 13/04/2018) to include the DPA (2018) and GDPR regulations, particularly the right to be forgotten and right to erasure.	7.0	Mary Umoh

1.0 Introduction and Scope

Tower Hamlets Council (The Council) processes Personal Data and recognises that appropriate and lawful treatment of Personal Data will help to enable successful delivery of services whilst maintaining confidence and integrity in the council.

The UK General Data Protection Regulation (“UK GDPR”) and the Data Protection Act 2018, together known as the “Data Protection Legislation”, govern the processing of Personal Data in the UK. Any organisation that processes Personal Data in the UK must comply with the Data Protection Legislation.

This Policy sets out the principles which The Council must follow when processing Personal Data. The Policy applies to all permanent and fixed term contract employees as well as consultants, contractors, casual and agency staff including secondees, collectively known as staff that process Personal Data in their role with the council.

All terms within the Policy are defined in Section 10.

2.0 Data Protection Principles

The Data Protection Legislation sets out the principles with which organisations must comply when processing Personal Data. It is the council’s policy to comply with these principles when processing Personal Data. The principles require that Personal Data must be:

- processed lawfully, fairly and in a transparent manner in relation to individuals (“lawfulness, fairness and transparency”)
- processed for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (“purpose limitation”)
- 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 (“accuracy”)
- kept in a form which permits identification of data subjects no longer than is necessary for the purposes for which the Personal Data is processed (“storage limitation” or “data 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”)

Furthermore, the council shall be responsible for, and be able to demonstrate compliance with these principles (“accountability”). Below, the Policy sets out the steps taken by the council and the action(s) that must be taken to comply with the principles:

2.1 Lawfulness, fairness, and transparency

The council must identify a valid lawful basis for each Processing Activity that involves processing Personal Data. The valid lawful bases are set out in the Data Protection Legislation. The Activity Owner, with the advice of the Information Governance, is responsible for ensuring that they have a valid lawful basis which is documented in the Record of Processing Activities (ROPA) prior to commencement of the Processing Activity. Please contact Information Governance for further information on the ROPA process.

The council must process Personal Data in a way that does not breach the law and is not unduly detrimental, unexpected, or misleading to the individuals concerned. Conducting a Data Protection Impact Assessment (“DPIA”) on high-risk activities helps to assess the impact of the Processing Activity on the Data Subjects and reduce the risk of detriment and unexpected or misleading activities. All activities must be assessed to determine whether a full DPIA is required, in accordance with the Data Protection Impact Assessment Procedure.

The council must be clear, open, and honest with Data Subjects about how their Personal Data will be processed. The council uses the Privacy Notices referenced in the Council Privacy Notice Log to explain how the applicable Data Subject’s Personal Data will be processed.

The appropriate Privacy Notice must be provided to the Data Subject at the point the Personal Data is collected from them. If Personal Data is obtained from a Third Party, the appropriate Privacy Notice must be provided to the Data Subject within a reasonable period and no later than one month after the Personal Data was collected.

2.2 Purpose Limitation

The council must be clear about what the purposes for processing the Personal Data are. These purposes must be documented (see Section 2.1) and provided to Data Subjects by way of the applicable Privacy Notice (see Section 4.1).

The Council must only use Personal Data for a new purpose if it is compatible with the original purpose for processing, consent is obtained or where there is a clear obligation set out in law.

2.3 Data Minimisation

The council must ensure that the Personal Data processed is sufficient to fulfil the purpose for which it was collected. The Personal Data must also have a relevant and rational link to that purpose and must be limited to what is necessary to fulfil the purpose (i.e., the Personal Data processed is not excessive or unnecessary). Staff must, as a minimum, only have access to the Personal Data that they need in order to perform the duties of their role, in accordance with the Records Management Policy.

2.4 Accuracy

The council must take all reasonable steps to ensure that Personal Data is accurate where possible, kept up to date and not misleading as to any matter of fact. Where Personal Data is discovered to be inaccurate or misleading, reasonable steps must be taken to correct the inaccuracies as soon as possible

2.5 Storage Limitation and Data Retention

The Council must not keep Personal Data for longer than it is needed for the purpose(s) for which it is being processed. The length of time and the justification for the retention of the Personal Data must be documented. For further information, please see the council's Records Management Policy.

2.6 Integrity and Confidentiality

The council must implement appropriate technical and organisational measures to maintain the security and confidentiality of Personal Data. The council's Records Management Policy, describes the appropriate security controls that should be applied to all types of information, including Personal Data, that the Council processes.

2.7 Accountability

The council must take accountability for complying with the Data Protection Legislation and must be able to demonstrate compliance with the requirements by:

- Adopting and implementing appropriate policies to comply with the principles of the Data Protection Legislation
- Implementing written contracts with Data Processors that require compliance with the requirements of Article 28 (3) of the UK GDPR. Colleagues responsible for selecting and/or onboarding a supplier must refer to the Procurement Policy
- Documenting and maintaining the ROPA carried out by the Council (please contact Information Governance for further information on the ROPA)
- Implementing appropriate security and organisational measures (see Section 2.6)
- Recording and, where appropriate, reporting Personal Data breaches in accordance with our Personal Data Breach Procedure
- Carrying out and documenting DPIAs for processing activities that are likely to result in high risk to data subjects' interests. All activities must be assessed to determine whether a DPIA is required, and Activity Owner is responsible for ensuring that this happens by way of the Data Protection Impact Assessment Procedure
- Providing appropriate and regular training and awareness communications to all colleagues regarding the requirements of the Data Protection Legislation and recording completion of such training; and
- Documenting the justification and analysis of why appointing a Data Protection Officer is / is not required for The Council.

These obligations are ongoing and must be reviewed on a regular basis as they will help the council to build trust and confidence with Data Subjects and will help to mitigate the risk of enforcement action(s) from the Regulator.

If you have any questions about any of the principles, policies, processes, or procedures mentioned above, please get in touch with the Information Governance Team at DPO@towerhamlets.gov.uk

3.0 Roles and Responsibilities

3.1 Chief Executive

Is ultimately responsible for ensuring the application of effective information security measures, delegating information security roles and responsibilities to the Corporate Leadership Team and other entities as follows:

3.2 Senior Information Risk Owner (SIRO)

Is responsible for managing the Council's risk, including maintaining and reviewing the Council's information risk register.

3.3 Information Asset Owner (IAO)

as custodians of information within their specific areas of business, are responsible for the information security management of their own records and for ensuring staff have the knowledge and skills to fulfil their information security responsibilities.

3.4 Head of Information Security

Is responsible for reporting and management of technology centred information security incidents in line with Information Security Policy, continuous risk assessment of IT services and effectiveness of applied mitigation controls.

3.5 Head of Information Governance

Is responsible for the overall governance of all aspects of information handling, including raising awareness and providing training to council staff and monitoring compliance.

3.6 Data Protection Officer

Is primarily responsible for advising on and assessing the council compliance with the DPA and UK GDPR and making recommendations to improve compliance.

3.7 All Managers

Are required to assist in the IAO responsibility set out above.

3.8 All Staff, Contractors, and Authorised Third Parties

All staff that process Personal Data during their role with the council must ensure that they carry out their duties in accordance with the principles and requirements of the policy by taking the following actions:

- Notifying Information Governance immediately following receipt of a Subject Rights request or query about Data Subject Rights by emailing ICWFOI@towerhamlets.gov.uk (see Section 4)
- Reporting any suspected Information Security Incidents immediately to cybersecurity@towerhamlets.gov.uk (see Section 4)
- Reporting any suspected breaches of the Policy to DPO@towerhamlets.gov.uk (see Section 6)
- Completing Data Protection training modules as required and
- Considering whether they are responsible for an activity that involves processing Personal Data ("Processing Activity") and, if so, ensure that the requirements for Activity Owners are carried out (see below).

Staff who have day to day or ultimate responsibility for a Processing Activity (“Activity Owner”) are responsible for ensuring that the requirements of the Policy are applied to their activities by taking the following actions:

- Documenting their activities involving Personal Data in the ROPA (please contact Information Governance for further information)
- Ensuring that their activities, including any changes to the activities, are assessed by the Information Governance to determine whether a Data Protection Impact Assessment is required, in accordance with the Data Protection Impact Assessment Procedure
- Deleting Personal Data, or ensuring that Personal Data is deleted, at the end of the relevant retention period, in accordance with the Data Asset Management Policy; and
- Ensuring that appropriate technical and organisational security measures are implemented in relation to their activities, in accordance with the Records Management Policy.

Information Governance is responsible for the implementation, operation, and review of appropriate controls to manage the risks associated with this policy. More information about the Key Controls can be found in Section 5.

The Council are responsible for the approval and adoption of the Policy. The Head of Information Governance is responsible for the Data Protection Policy and for the implementation of additional controls to mitigate the Data Protection risk.

4.0 Data Subject Rights

The Data Protection Legislation provides rights to Data Subjects in relation to their Personal Data and how it is processed by the council. In certain circumstances, a Data Subject may have any of the following rights:

- *The right of access (often referred to as a “Subject Access Request” or “SAR”)* – this provides the right for a Data Subject to access a copy of the Personal Data processed about them.
- *The right to be informed* – Data Subjects have a right to be informed about the collection and use of their data, including the purposes for processing, retention periods and recipients of their Personal Data.
- *The right to rectification* – if a Data Subject believes that The Council is processing inaccurate or incomplete Personal Data about them, they can request the inaccuracy to be rectified or completed.
- *The right to erasure (often referred to as “the right to be forgotten”)* – a Data Subject may request that Personal Data processed about them by The Council is deleted.
- *The right to restrict processing* – this right provides the Data Subject an entitlement to limit The Council to only processing their Personal Data for certain purposes.
- *The right to portability* – a Data Subject may request to have their Personal Data transferred to another organisation or to themselves for use across other services.
- *The right to object* – Data Subjects may have the right to object to The Council processing their Personal Data, which would require The Council to stop processing their Personal Data. This right is absolute where it is in relation to Personal Data processed for Direct Marketing.

- *The right to object to automated decision making or profiling* – Data Subjects have the right to object to decisions made by entirely automated means or automated profiling. This right requires a human to review the decision or profiling that was previously automated.

Requests made in relation to these rights can be made in any form (e.g., written, email and verbal) and do not necessarily need to use the formal language or refer to the right by name. The Council must respond to such requests within one calendar month from receipt of a valid request.

If you have received a communication that you believe may relate to one of the above rights, you must notify the Information Governance immediately at ICWFOI@towerhamlets.gov.uk

5.0 Data Protection by design and default

The UK GDPR requires the Council to integrate data protection concerns into every aspect of our activities that involve Personal Data. This means that the Council must put in place appropriate technical and organisational measures to implement the data protection principles (see Section 2) effectively and to integrate safeguards in order to meet the Data Protection Legislation's requirements and protect Data Subjects' rights (see Section 4.1).

The Council must ensure that privacy and data protection issues are considered at the design stage of any new or changed system, service, product, or process that involves Personal Data. Activity Owners are responsible for ensuring that their activities are assessed against these requirements via the Data Protection Impact Assessment Procedure. Please contact the Data Protection Team for further information at DPO@towerhamlets.gov.uk

6.0 Personal Data Incidents and Breaches

During the course of any organisations' activities, an Information Security Incident that involves Personal Data (a "Personal Data Incident") is likely to occur. As defined by the Information Security Incident Management Process, an Information Security Incident is one or multiple related and identified information security events that meet established criteria and can harm an organisation's assets or compromise its operations.

A Personal Data Incident may lead to a Personal Data Breach. A Personal Data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The Council must, in certain circumstances, report a Personal Data Breach to the Information Commissioner (ICO) within 72 hours of becoming aware of the Personal Data Breach.

The Information Governance Team is responsible for assessing each Personal Data Incident to determine whether a Personal Data Breach has occurred and are responsible for notifying the Regulator and Data Subjects, where required or appropriate, in accordance with the Personal Data Breach Procedure.

All council colleagues must report any suspicion of an Information Security Incident to cybersecurity@towerhamlets.gov.uk. Please see the Information Security Incident Management Process for further information.

7.0 Key Controls

Control name	Control objective	Control timing / application	Control operator
Personal Data Incident Procedure	To reduce the risk of (i) The council not complying with the data breach requirements from the UK GDPR and DPA; and (ii) harm to the individuals affected by the incident. The key control ensures that data incidents involving personal data are reported to, investigated, and assessed by the Data Protection Team.	Upon receipt of notification of a personal data incident	DPO
E-learning training for all staff	To ensure that all staff are aware of the requirements of this policy and how to comply	Upon commencement of their role with the council and at least annually thereafter.	Information Governance Team
Data Protection Impact Assessment Procedure	To (i) identify activities that require a DPIA due to their high-risk nature (ii) identify the risks associated with that activity and (iii) identify actions to mitigate the risks identified.	As required when a new and/or changed activity, project, system etc that involves personal data is proposed	DPO
Data Subject Rights Procedure	To (i) ensure the subject rights requests are responded to within the regulatory timelines (one month) and (ii) ensure that the right actions are taken in response to the request.	As required when a request has been received	Information Governance Team

8.0 Compliance Monitoring

The Information Governance Team are responsible for monitoring compliance with this Policy. Compliance with the Policy will be monitored and assessed as part of the Information Governance's monthly Key Risk Indicator Quality Review process.

Council Staff who breach this Policy may face disciplinary action, which could result in dismissal for misconduct or gross misconduct. Please report any suspected breaches of the Policy to the Data Protection Officer at DPO@towerhamlets.gov.uk

The second line of defence shall monitor the effectiveness of Policy controls on a risk-based approach, evidenced in the annual Compliance monitoring programme.

9.0 Training

All Council Colleagues must complete the Data Protection e-Learning module upon commencement of their role with The Council and at least annually thereafter. The Compliance Team are responsible for reporting on completion of the e-Learning module.

10.0 Who to contact for further help

If you have any queries or questions about the Policy or its requirements, please contact the Data Protection Officer at DPO@towerhamlets.gov.uk

11.0 Definitions

The terms that appear in the Policy shall have the definitions outlined below. Any undefined terms in the Policy shall have the definitions provided in the Council's [Business Glossary](#).

Activity Owner – the individual responsible for a Processing Activity.

Staff - all permanent and fixed term contract employees as well as consultants, contractors, casual and agency staff including secondees.

Data Protection Legislation – collective name for the Data Protection Act 2018 and the UK General Data Protection Regulation.

Data Subject - any individual person who can be identified, directly or indirectly from the Personal Data.

Personal Data - means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal Data Breach - a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data. The Council must, in certain circumstances, report a Personal Data Breach to the Regulator within 72 hours of becoming aware of the Personal Data Breach.

Processing Activity - any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction.




Profiling - any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location, or movements.

Special Category Data - personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

12.0 Policy Review

This policy will be reviewed and updated alongside other information governance policies on a regular basis, not to exceed 12 months.

13.0 Policy Signoff

Role		Name	Date
Approver		Raj Chand Director of customer services	12/09/2022
Reviewer		Adrian Gorst Director of IT (SIRO)	23/9/2022
Reviewer		Muhammad Forhad (DPO)	26/9/2022