Data Protection Policy

Introduction

The processing of personal data is essential to many of the services carried out by the Council, and this policy sets out how it complies with the UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA) and other related legislation.

It should be read in conjunction with the supporting policies and other documents listed in Annex A. There is a glossary of terms in Annex B.

Purpose

This Policy sets out how the Council will comply with data protection legislation: UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018 (DPA) and related laws.

Compliance with them reduces the likelihood of an information security breach and its wider effects, including causing harm/distress to data subjects, reputational damage, substantial financial penalty and scrutiny from the Information Commissioner's Office.

Since the delivery of many of the Council's services and functions are reliant on the processing of accurate and usable personal data, adherence to the legislation will improve efficiency and effectiveness in the public interest and maintain the trust of all residents and service users.

Scope

The Council is registered with the Information Commissioner's Office (ICO) as a "Data Controller" (Registration No Z4600177) and this Policy applies to the processing of all

personal data including the collection, use and sharing of personal data where the Council is the Data Controller or the Data Processor and when it is a joint Data Controller.

It applies to everyone working for the Council, including agency staff and contractors regardless of who created the data, where it is held or the ownership of the equipment on which it is held. Mandatory training is provided to staff to assist them in meeting their obligations under this Policy.

Elected members are Data Controllers and are responsible for the personal data that they collect, store, use and delete.

Data Protection Principles

The following key principles underpin this policy statement, and the Council will comply with them by putting in place measures to ensure that personal data is:

- processed lawfully, fairly and in a transparent manner in relation to the data subject **("lawfulness, fairness and transparency")**

- collected and created 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 those purposes **("data minimisation")**

- accurate and, where necessary, kept up to date **("accuracy")**

- retained for no longer than is necessary **("storage limitation")**

- kept safe from unauthorised access, accidental loss or deliberate destruction **("integrity and confidentiality")**

  and

- that the Council can demonstrate that it has done so **("accountability")**

To maintain these principles the Council will:

2

- Let data subjects know how and for what purpose their personal data is being processed by means of a “Privacy Notice”

- Inform data subjects if their personal data will be shared and why and with whom when there is a legitimate purpose for doing do

- Only process personal data where there is a lawful basis to do so

- Only re-use personal data where there is a valid reason or basis for doing so, for example in connection with research and analysis, where the new use has been assessed as being compatible with the original purpose for which the data was provided or where specific consent has been provided.

- Check the quality and accuracy of the information it holds and make it easy for data subjects to do so

- Ensure that information is not held for longer than necessary and that such information is destroyed appropriately and securely

- Have safeguards in place to protect personal information in all formats from loss, theft or unauthorised disclosure

Lawful basis for Processing
The grounds for processing personal data are:

1. Required for the performance of a contract between the Council and the data subject
2. For tasks carried out in the public interest
3. To comply with the Council’s legal obligations
4. Vital interests – to protect or save an individual’s life
5. Consent

Guidance from the ICO states that*: “no single basis is “better” or more important than the others, all are equally valid; when choosing which to rely on, the most appropriate basis to use depends on the purpose for which the data is being processed and the relationship with the individual.”*

In order to fulfil our statutory responsibilities as a Local Authority, in most cases the lawful basis for processing personal data will be to perform a task carried out in the public interest and to comply with the legal obligations set out in law. This includes for example: providing an Electoral Service; administering Council Tax; delivering services related to Education and Learning; and the prevention of crime.

3

The Council will only ask for consent if consent is the only lawful basis for the purpose of the processing of personal information and if it is not doing so under one (or more) of the other four legal basis for processing. For example: residents agreeing to a particular method of communication such as receiving emails about local events. Consent can be withdrawn at any time.

Special Category (formerly known as Sensitive Personal Data)
Where special category personal data is processed the Council will also ensure that one of the additional conditions set out the legislation is met, together with any further requirements set out in other legislation.

Sharing Information
The Council is legally obliged to share certain data with other public bodies, such as central Government Departments, when required to do so. It is also required to safeguard public funds to prevent fraud and it may share data with other public bodies for this purpose.

The Council has also appointed external agencies, companies or other organisations to carry out services on its behalf, including, for example: Street Cleansing; Highway Maintenance; Recycling and Waste Collection; and payment processing.

Each service provider will be required to demonstrate, via a written contractual agreement, that Council-controlled personal data will be handled in compliance with data protection legislation, and they have put appropriate technical and organisational measures in place. This data sharing is in accordance with our Privacy Notice(s) which can be viewed at:
https://www.wandsworth.gov.uk/the-council/open-data-and-transparency/privacy/wandsworth-council-privacy-notice/

In the event of an emergency or civil incident personal data may be shared with other organisations to fulfil our statutory duties and protect individuals from harm.

The Council carries out data matching exercises to ensure the safeguarding of public money and to minimise levels of fraud in addition to ensuring it delivers services and assistance to those entitled to receive them. Data matching exercises will only be carried out for specific lawful purposes and will comply with relevant Codes of Practice.

Cabinet Office
https://www.gov.uk/government/publications/code-of-data-matching-practice-for-nationalfraud-initiative

4

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_dat a/file/750372/Code_of_Data_Matching_Practice.pdf

Rights of individual data subjects
The Council will uphold individual data subject rights, including the right to:

- be provided with specified information about the Council's processing of their personal data **(the right to be informed)**
- access their personal data **(the right of access)**
- have their personal data rectified if inaccurate or incomplete **(the right of rectification)**
- have, subject to legal obligations, their personal data deleted or removed **(the right of erasure)**
- in certain circumstances **the right to restrict processing** including where you have identified inaccurate information
- **the right to object** to the processing of your personal information.
- in certain circumstances, to move personal data that the individual has provided to the Council to another organisation **(right of data portability)**
- not be subject to a decision based solely on automated decision making and processing **(rights related to automated decision making, including profiling)**

For further information on the Rights of Individual Data Subjects see our Individual Rights Policy.

As required by law, the Council has appointed a Data Protection Officer whose role includes ensuring that appropriate policies and processes are in place so that these rights can be exercised according to the provisions of the legislation.

When a data subject exercises one of these rights, the Council will respond without undue delay and within the statutory time limits following proof of identification.

5

Information Security
The Council has put in place appropriate security measures to prevent unauthorised processing of personal data and against the accidental loss of or damage to personal data from the point of collection to its destruction. These measures are continually updated so that the Council maintains confidentiality, integrity and availability of personal data at all times.
In the event of a personal data breach occurring, this can be reported by means of the following link to the Council's web site where more information can be found with some examples of what might constitute a personal data breach:
https://www.wandsworth.gov.uk/the-council/open-data-and-transparency/privacy/report-a-data-breach-or-a-security-incident/

Data Protection Impact Assessments (DPIA)
The Council will conduct a DPIA, where there is a high risk to the rights and freedom of individuals in order to assess and mitigate identified risks relating to new systems or a new business process for example.

International Transfers of Data

Generally, the Council will not process your personal data outside of the UK or the EEA. In exceptions where we do, we will ensure equivalent data protection controls are in place.

Complaints
Complaints regarding the processing of personal data should be made to the Data Protection Officer. For example: when personal data has not been handled securely; that information has not been obtained fairly; or that personal data had been retained for longer than was necessary.

Details of the Council's Data Protection Complaints Procedure can be found here: Data protection complaints procedure - Wandsworth Borough Council

Changes to this Policy
The Information Governance Strategic Board (IGSB) has authorised the Data Protection Officer to review this Policy regularly and, taking into account changes in legislation, amend accordingly. The Board will review the Policy annually.

Feedback on this Policy
If you have any questions or comments about this policy or have suggestions for how it might be improved or if you wish to contact the Council's Data Protection Officer, you can email to:

DPO@richmondandwandsworth.gov.uk

6

Or write to the Data Protection Officer at The Town Hall, Wandsworth High Street, London SW18 2PU

January 2023.

Annex A
Links to other policy documents (Internet only)

https://www.wandsworth.gov.uk/the-council/open-data-and-transparency/accessing-information/accessing-your-personal-information-subject-access-request/
Subject Access Request

https://www.wandsworth.gov.uk/the-council/open-data-and-transparency/privacy/request-restriction-of-personal-data/
Request restriction of personal data

https://www.wandsworth.gov.uk/the-council/open-data-and-transparency/privacy/request-erasure-of-personal-data/
Request erasure of personal data

https://www.wandsworth.gov.uk/the-council/open-data-and-transparency/privacy/wandsworth-council-privacy-notice/
Wandsworth Privacy Notice

https://www.wandsworth.gov.uk/the-council/open-data-and-transparency/privacy/departmental-privacy-notices/
Departmental Privacy Notices

https://www.wandsworth.gov.uk/the-council/open-data-and-transparency/privacy/records-management/
Records Management Policy

7

Annex B

Glossary

- *'Personal data'* is any information relating to an identified or identifiable natural person, either through their name or another identifier such as 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

- *'Processing'* refers to any operation performed on personal data, whether or not by electronic or automated means, such as collection, use, storage, recording, organisation, structuring, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

- *'Data subject'* is the term used to describe any given person when identified in relation to their personal data

- *'Data controller'* is the organisation that determines the purposes for which, and the manner in which, any personal data is processed. They are responsible for establishing practices and policies in line with data protection legislation.

- '*Joint Data Controller'* are the organisation that, acting together with another, decides the purposes and manner in which personal data is processed

- *'Data Protection Officer'* (DPO) assists the Council monitor internal compliance, informs and advises on data protection obligations and acts as a contact point for data subjects and the supervisory authority

- *'Information Governance Strategic Board' (IGSB)* has responsibility for the Information Governance and Security arrangements across the Council and oversight of compliance issues reported to it

- *'Personal data breach'* means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

8

- *'Special categories'* of personal data encompasses ethnicity and data concerning health, among other categories. To process these, there are extra requirements. Similar requirements exist in the GDPR for processing data on criminal convictions or offences.

- *'Information Commissioner's Office'* (ICO) The ICO is the UK's independent body set up to uphold information rights and the Department for Digital, Culture Media and Sport is the ICO's sponsoring department within Government

---

Document Name	Data Protection Policy
Version No.	3 (January 2023)
Status	Approved
Owner	Information Governance Manager
Approved by	IGSF (10 January) and IGSB (18 January) 2023.

If this document is in printed format it may not be the current version. Before subsequent use check the documents version number on the intranet.

Document Control

This document should be reviewed annually by the document owner and a note made to this effect in the table below

Change Control Table

Version	Description	Who By	Release Date
1	Original Policy	IG Manager	February 2020
2	Minor revisions	IG Manager	November 2021
3	Various up-dates	IG Manager	January 2023

9

10