CITY OF WOLVERHAMPTON COUNCIL

Data Protection Policy

DP00

wolverhampton.gov.uk

Version History

Version	Date	Description	Author, Role
1.0	22/03/2012	Draft for consultation with ICO project group	Anna Zollino-Biscotti -
1.1	11/12/2012	Revised following IG Board submission and audit review	Charlotte Johns
2.0	18/12/12	Policy approved by Cabinet (Resources) Panel	
2.1	24/03/16	Revised Approved by IG Board	Iain Harrison
3.0	26/02/18	Revised following law changes	Anna Zollino-Biscotti, Kate Collins
3.1	19/04/18	Revised following IG Board review	Kate Collins
3.2	04/07/19	Annual Review	S Taylor
3.3	16/08/2021	Review following restructure of IG policy framework	IG Team
4.0	17/02/2022	Approval from members of the IG Board and SEB	IG Team
5.0	05/12/2023	Scheduled review	Information Governance Team

Table of Contents

Introduction 3

Legal and Regulatory Obligations for the Council 3

Scope 3

Principles of Data Protection 4

- Lawfulness, fairness and transparency 4
- Used for specified, explicit purposes (Purpose Limitation) 4
- Used in a way that is adequate, relevant, and limited to only what is necessary (Data Minimisation) 4
- Accurate and, where necessary, kept up to date 4
- Kept for no longer than is necessary (Storage limitation) 4
- Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage 5

Individual Data Rights 5

- The right to be informed 5
- The right of access 5
- The right to rectification 5
- The right to erasure 5
- The right to restrict processing 5
- The right to data portability 5
- The right to object 6
- Rights in relation to automated decision making and profiling. 6

Roles and Monitoring 6

- DPO 6
- Other Roles 6
- Monitoring 6

Training and dissemination 6

Definitions 7

Links to other Policies 7

Introduction

The City of Wolverhampton Council (CWC) collects and uses different types of information about people with whom it deals and communicates with in order to operate. These include current, past, and prospective employees, Councillors, contractors, suppliers, service users and carers. In addition, it may occasionally be required by law to collect and use certain types of information to comply with the requirements of government departments for business data.

The purpose of this policy is to enable CWC to:

- Comply with the law in respect of the personal and special category data it holds about individuals.
- Follow good practice.
- Protect the Council's customers, service users, staff, and other individuals who the Council holds personal information about.

This policy will provide a framework within the Council to ensure compliance with current Data Protection law and associated legislation relating to personal information.

CWC recognises its responsibility to fully implement its duties in respect of the above and to ensure that all its employees understand and can implement all the requirements of the Data Protection Act 2018 (DPA), and the UK General Data Protection Regulations 2016/679 (UK GDPR).

This policy will underpin any operational processes and procedures connected with the principles of Data Protection. This policy is a key policy in the Information Governance Framework.

Legal and Regulatory Obligations for the Council

The Data Protection Act 2018 (DPA), and the UK General Data Protection Regulations 2016/679 (UK GDPR) detail the principles, requirements, and safeguards for personal data. It is the Council's obligation, as Data Controller, to ensure compliance with current Data Protection laws and regulations.

These pieces of legislation must be applied to ensure the rights and freedoms of living individuals are not compromised, and data is processed in an appropriate and secure manner. They stipulate that those who record and use personal information must be open about how the information is used and must follow good information handling practices. It applies to the whole life cycle of information, including the collection, use, disclosure, retention, and destruction of data.

Scope

This policy applies to all personal and special category data held by the Council and includes manual/paper records within relevant filling systems, as well as personal data that is electronically processed by computer systems or other means such as

CCTV systems.

This policy will apply to anyone accessing or using Council data, including for example: employees, temporary or contract staff, volunteers, work placements, Council members, contractors, suppliers, services providers, or other partner agencies.

Principles of Data Protection

The Council will ensure its practices are compliant with the data protection principles, as follows:

Lawfulness, fairness, and transparency

- The Council will identify a valid legal basis under UK GDPR for collecting and using personal data.
- The Council will collect and use personal data in a way that is fair and expected.
- The Council will be clear, open and honest with people from at point of collection, about how we will use their personal data, including providing a Privacy Notice.

Used for specified, explicit purposes (Purpose Limitation)

- The Council will only collect and process personal information to fulfil operational needs or to comply with any legal requirements.
- The Council will only process personal data for a new purpose if either this is compatible with the original purpose, or where we have a clear legal obligation or your consent.

Used in a way that is adequate, relevant, and limited to only what is necessary (Data Minimisation)

The Council will make sure the personal data we use is:

- Adequate – sufficient to properly fulfil our stated purpose;
- Relevant – has a rational link to that purpose; and
- Limited to what is necessary – we will not hold more than we need for that purpose.

Accurate and, where necessary, kept up to date

- The Council will take all reasonable steps to ensure the personal data we hold is not incorrect or misleading as to any matter of fact.
- If we discover or are notified that personal data is incorrect or misleading, we will take reasonable steps to correct or erase it (where we are legally allowed to) as soon as possible.

Kept for no longer than is necessary (Storage limitation)

- The Council will not keep personal data for longer than we need it.
- The Council will maintain a retention schedule for how long to keep documents, based on other relevant laws and guidance or best practice.

- The Council will consider keeping anonymised information which has an enduring historical value for public interest archiving, scientific or historical research, or statistical purposes.

Handled in a way that ensures appropriate security, including protection against unlawful or unauthorised processing, access, loss, destruction or damage

- The Council will put in place appropriate technical and organisational security measures to protect the personal data we hold to maintain its integrity and confidentiality.
- Ensure that personal information is not transferred abroad without suitable safeguards.

Individual Data Rights

The UK GDPR provides the following rights for individuals in relation to their personal data. The Council has processes in place to manage these requests and comply with their responsibilities under the law.

The right to be informed

The Council will be clear, open and honest with people from at point of collection, about how we will use their personal data, including providing a Privacy Notice

The right of access

Individuals have the right to request a copy of the data the Council holds about you.

The right to rectification

Individuals have the right to request that inaccurate personal data is rectified or completed if it is incomplete.

The right to erasure

Individuals in some circumstances have the right to request their data is erased. Individuals will be informed if there is a legal reason that means personal data cannot be deleted.

The right to restrict processing

Individuals have the right to request the restriction or suppression of their personal data. This is not an absolute right and only applies in certain circumstances.

The right to data portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services.

The right to object

Individuals in some circumstances have the right to object to the processing of their personal data. Individuals will be informed if there is a legal reason that means the personal data must be processed by the Council. Individuals have an absolute right to stop their data being used for direct marketing. Individuals can usually set their marketing preferences within their online accounts.

Rights in relation to automated decision making and profiling.

If an automatic decision has been made about an individual by a computer, they have the right to request human intervention or challenge a decision.

The supplementary information individuals are entitled to about their data is available in the Council Privacy Notice(s). Individuals can contact the Council if they are concerned about their personal data, or to make a data rights request here.

Roles and Monitoring

DPO

The Council is required by Data Protection laws to have a Data Protection Officer (DPO) in place, who ensures, in an independent manner, that the organisation applies the laws to protecting individuals' personal data by audit and monitoring.

Other Roles

Please find a description of other relevant roles and responsibilities here: What is Information Governance? | City Of Wolverhampton Council

Monitoring

This policy will be approved and monitored by the Councils Information Governance Board. It will be reviewed every 2 years or sooner if legislative changes require.

Training and dissemination

The Council will ensure that everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice.

All relevant staff are mandated to complete the Councils protecting information training upon induction and are required to update their training on this subject matter on a regular basis.

Specialised training will be made available to staff where their role requires them to handle higher volumes of personal data or data that is more sensitive in nature.

This policy is supplemented with detailed guidance for staff which must be followed.

This policy and any associated staff guidance will be disseminated to Council staff via the Council's intranet site, internal news articles, and via Operational Managers Network. The policy will be made available to staff and the public on the Council's Public Website.

Definitions

Please find a description of common Information Governance Key terms here: What is Information Governance? | City Of Wolverhampton Council

Links to other Policies

This Policy forms part of the Information Governance Framework, and should be read in conjunction with the other related policies within the framework which can be found What is Information Governance? | City Of Wolverhampton Council and are as follows:

- IG00 Strategy
- AI00 Access to Council Information
- IS00 Information Security Policy
- RM00 Records Management Policy
- Information Governance Definitions, Roles and Responsibilities