LAW ENFORCEMENT (DATA PROTECTION) POLICY

V. 1.0
Date:

1. Introduction

This Policy explains what special requirements the Council must meet with processing Personal Data relating to criminal offences (including the suspected and alleged commission of offences) and how staff can comply with those requirements when carrying out their work. The Policy also satisfies the requirement in the Data Protection Act 2018 (DPA 18) for a Data Controller to have in place an 'appropriate policy document' in these situations.

2. Definitions

Anti-fraud organisation – any unincorporated association, body corporate or other person which enables or facilitates any sharing of information to prevent fraud or a particular kind of fraud which has any of these functions as its purpose or one of its purposes. [1]

Data Protection Legislation – the General Data Protection Regulation (Regulation (EU) 2016/679), the Law Enforcement Directive (LED), the Data Protection Act 2018 (DPA 18 – as amended) and any regulations that apply to any of the specified legislation.

Processing – an operation or set of operations which is performed on personal data, or on sets of personal data, such as:
collection, recording, organisation, structuring or storage,
adaptation or alteration,
retrieval, consultation or use,
disclosure by transmission, dissemination or otherwise making available,
alignment or combination, or
restrictions, erasure or destruction

Competent authority – either a body specified in schedule 7 of the Act (Local Authorities are not included here) or *'any other person if and to the extent that the person has statutory functions for any of the law enforcement purposes'.*

Law enforcement purpose – the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. This definition includes the alleged commission of criminal offences by the data subject.

Sensitive data – processing of any of the below by a competent authority for law enforcement purposes:

- Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership;
- Genetic or biometric data, for the purpose of uniquely identifying an individual;
- Data concerning health; or
- Data concerning an individual's sex life or sexual orientation.

3. Scope

[1] Section 68(8) of the Serious Crime Act 2007

There are three strands to processing personal information for the purpose of preventing and detecting the commission of offences

- Where the Council is a competent authority (i.e. is performing a statutory function) in relation to criminal offences and penalties;

- Where the Council is not a competent authority (i.e. is not performing a statutory function) in relation to criminal offences and penalties, and,

- Where the information relates to civil offences and penalties.

This Policy applies to the first two of these strands (i.e. processing of any personal data relating to criminal offences and penalties). Information relating to civil offences must be processed as personal data under the Data Protection Policy.

This Policy should inform the activities of ALL members and officers of Wycombe District Council and third party organisations working on behalf of the Council.

3.1 Is the Council a competent authority?

The Council will be a competent authority for the processing of some criminal offence data, but not others.

For example, the Council will be a competent authority for processing relating to environmental offences, as it holds statutory powers to enforce criminal law. It will not be a competent authority for the purpose of sharing information with the police force where the force is conducting an investigation and requests information from the Council (such as sharing used to be handled under section 29 of the Data Protection Act 1998).

The table below details which legislation and Council Guidance applies to each strand of processing:

Processing activity	Legislation	Council Policies
Where the Council is acting as a competent authority	Part 3 DPA 2018	Annex A to this Policy
Where the Council is not acting as a competent authority, but the information relates to a criminal offence	Parts 1, 2 and 3 of Schedule 1 DPA 2018	Section 5 of the Protecting Special Category Data Policy
Where the information relates to civil offences	GDPR	The Data Protection Policy and Protecting Special Category Data Policy

4. Aims

The aims of this Policy are:

- To ensure that all members and officer of Wycombe District Council, processors acting on the Council's behalf and third party organisations are aware of which data protection legislation applies to the processing they are conducting.

- To ensure that all members and officers of Wycombe District Council, processors acting on the Council's behalf and third party organisations are aware of the principles and lawful conditions that apply under each law.

- To explain the safeguards Wycombe District Council operates to secure compliance with the data protection principles and protect the rights and freedoms of data subjects when processing sensitive personal data relating to criminal offences and penalties (as required by section 42 of the DPA 2018), and,

- To identify the responsibilities of members, officers and third party organisations in complying with the law that applies in each instance of processing.

5. Law Enforcement Processing

The GDPR expressly does not apply to the processing of personal information by competent authorities for law enforcement purposes.[2] A separate piece of EU legislation[3] sets out the standards member states' own legislation must meet for this type of processing. In the UK this is achieved in part 3 of the DPA 2018.

Specifically, 'law enforcement processing' captures the processing by a competent authority of criminal offence and criminal penalty data wholly or partly by automated means or if the data forms, or is intended to form, part of a filing system.

5.1 Compliance with the data protection principles:

Where the Council is a competent authority processing information for a law enforcement purpose it must comply with the below Principles:

Processing must be lawful and fair, and meet one of the below conditions:

- Purposes of processing must be specified, explicit and legitimate;
- Personal data be adequate, relevant and not excessive;
- Personal data be accurate and up to date;
- Personal data be kept for no longer that is necessary; and
- Personal data be processed in a secure manner.

More information on each Principle is given below:

5.1.1 First principle – fair and lawful processing

Processing must not take place unless the reason for processing is derived from legal powers granted to the Council and it does not infringe data protection legislation or any other law.

Subjects must be told that their data is being collected, who is collecting it and what we will do with it. The Council makes this information available through privacy notices. A privacy notice must be in place and made available to the subject before any information is obtained from them. If personal information is not obtained from the subject directly a notice must be provided to them at the earliest of the below scenarios:

[2] Recital 19 and Article 2(2)(d) GDPR

[3] Directive (EU) 2016/680 – the Law Enforcement Directive

- At the date of the first communication with them or otherwise;

- If the data is to be disclosed to another recipient, before the date of disclosure; or,

- At the latest within one month.

If the law enforcement purpose would be prejudiced by notifying the subject of the processing of their data then an exemption from the above obligations may apply.

5.1.1.1 Processing conditions

In addition to being lawful and fair, one of the below conditions must also be met in all cases:

- The data subject has given their consent to the processing, or

- The processing is necessary for the performance of a task carried out for the law enforcement purpose by a competent authority.

5.1.1.2 Processing conditions (sensitive data)

Processing of sensitive data for a law enforcement purpose will be lawful only if:

Explicit consent has been gained from the subject, or

The processing is strictly necessary for the law enforcement purpose and meets one of the further conditions from Schedule 8 (see Annex A)

In both cases the Council must have in place an appropriate policy document [4]

5.1.2 Second principle – processing purpose

Personal data collected for a law enforcement purpose must be specified, explicit and legitimate.

Personal data can be processed for a further purpose, but no processing must be carried out on it that is incompatible with the initial processing purpose. To be compliant with this principle the Council must be authorised by law (i.e. have powers to enforce the criminal law) to process for the further purpose, and the processing must be necessary and proportionate to that purpose.

For example, information collected for the purpose of a trading standards investigation must not be used for the incompatible purpose of sending marketing material.

5.1.3 Third principle – relevancy

The information collected and processed for the law enforcement purpose must be adequate, relevant and not excessive for the purpose it is collected.

[4] Defined in section 42 DPA 2018

Only the minimum amount of information necessary for the purpose in question must be processed (e.g. shared, collected or requested).

5.1.4 Fourth principle – accuracy

The personal data must be accurate and kept up to date. Where compatible with the processing purpose, inaccurate data should be erased or rectified as soon as it is found to be incorrect.

A distinction between the data relating to the below categories of individuals must be made:

- Suspects
- Those convicted of criminal offences
- Victims; and
- Witnesses or those with information about offences.

5.1.4.1 Intelligence

It is also a requirement of the law that, so far as possible, personal data based on personal assessment and opinion (including intelligence) be distinguished from that which is based on fact.

5.1.4.2 Sharing data

Inaccurate, incomplete or out of date information must not be shared for any law enforcement purpose. To that end:

- Personal data must be verified before being shared;
- An assessment of the accuracy, completeness and reliability of the data must be included when data is shared; and,
- Recipients must be informed if personal data is found to be inaccurate or the sharing unlawful.

5.1.5 Fifth principle – retention

Personal data must be kept for no longer than is necessary for the law enforcement purpose. A suitable retention period must therefore be established to guide periodic reviews of the personal data held. These retention periods are defined in the Council's Retention Schedule and Information Asset Register.

Once this retention period has been exceeded the information must be deleted, unless further retention is justified in accordance with the Archiving condition (see Annex A).

Information must not be retained beyond the defined organisational retention period without these reasons being specified and recorded.

5.1.6 Sixth principle – data security

Information processed for a law enforcement purpose must be protected against unauthorised or unlawful processing and against accidental loss, destruction or damage. The Council's Information Security Policy sets out the security requirements.

5.2 Subject rights

Subjects have the following rights:

- To be informed of our use of their information;
- Of access to their information;
- Rectify information about them that is inaccurate;
- To have their information erased (the 'right to be forgotten');
- To restrict how we use their information;
- To move their information to a new data controller;
- To object to how we use their information;
- Not to have decisions made about them on the basis of automated decision making;
- To object to direct marketing; and,
- To complain about anything the Council does with their information.

The subject rights are limited in application and apply only in specific situations. They may also be restricted (in whole or in part) where they would conflict with the law enforcement purpose.

6. Safeguards – processing sensitive data

Article 10 of the GDPR requires that Member States provide safeguards for the rights and freedoms of data subjects in any national law they may enact to authorise the processing of personal data relating to criminal convictions and offences.

For this reason sections 35(4) and (5) of the DPA 2018 requires controllers (when processing criminal data) to have an appropriate guidance document in place. Section 42(2) further defines the content of such a policy, in that it should:

Explain how the Council will ensure compliance with the data protection Principles (described in section 5 above) and,

Explain the Council's policies as regards the retention and erasure of personal data processed in reliance on a particular condition, giving an indication of how long such personal data is likely to be retained (described in section 5.1.5 Retention above).

Be retained, reviewed and (if appropriate) updated from time to time (see section 7 below): and

Made available to the Information Commissioner on request (and without charge).

This Policy constitutes the appropriate policy document for processing under these conditions.

7. Review and Retention

7.1 Review

This Policy will be reviewed on an annual basis.

7.2 Retention

Each version of this Policy will be retained for a period of seven years from the date of approval.

ANNEX A

Further conditions for processing sensitive data for a law enforcement purpose are created by Schedule 8 of the DPA 2018. The most relevant to a local authority are:

Statutory purpose

The processing is necessary for the exercise of a function conferred on a person by an enactment and reasons of substantial public interest.

Vital interests

The processing is necessary to protect the vital interests of the data subject or of another individual.

This condition only applies in life and death situations – for example, sharing medical information with a hospital where the subject is unable to consent.

Legal claims

The processing is necessary for:

- The purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
- For the purpose of obtaining legal advice, or
- Is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

Preventing fraud

The processing (including disclosure) is necessary for the purposes of preventing fraud or a particular kind of fraud, and:

- The Council is acting as a competent authority as a member of an anti-fraud organisation, or
- In accordance with arrangements made by such an organisation.

Archiving

The processing is necessary for:

- Archiving purposes in the public interest; or
- Scientific or historical research, or statistical purposes.