Data Protection Policy

Version 7.0 - 2025

www.wyre.gov.uk

wyre council

Title	Data Protection Policy
Version number	v.7.0
Author(s) name & role title	
Owner name & role title	Joanne Billington, Assistant Director of Governance and Legal (Monitoring Officer)
Reviewer name & role title	Rachael Krier, Data Protection and Information Governance Officer

Date of creation	[2018]	Review cycle	Annual
Last review	2024	**Next review date**	October 2025

Version	Date	Section/reference	Amendment
v.7.0		Section 11.2; Sections 12, 14, 17, and Appendix A; Section 15.4-8 Sections renumbered and updated as follows Sections 2 – 6 Sections reordered Section 10 - 15	Removed and added to Risk Register; removed to Information Security Policy and updated; sections removed Scope amended; Purpose added; Legal Context updated; Roles and Responsibilities merged with other relevant sections; Definitions added Added and amalgamated existing content to demonstrate compliance with principles

1. Background

1.1. The processing of personal data is essential to many of the services and functions carried out by local authorities. Wyre Council ('the council') recognises that compliance with data protection legislation (including the UK General Data Protection Regulations ('GDPR'), the Data Protection Act 2018 ('DPA') and related legislation) will ensure that such processing is carried out fairly, lawfully and transparently.

1.2. Data protection legislation and Article 8 of the European Convention on Human Rights recognise that the processing of personal data needs to strike a balance between the need for an organisation utilising personal data to function effectively, efficiently and in the wider public interest, and respect for the rights and freedoms of the individual(s) ('data subject(s)') to whom the personal data relates. This policy sets out how the council intends to safeguard those rights and freedoms.

2. Scope

2.1. This policy applies to the collection, use, sharing and other processing of all personal data held by the council, in any format including paper, electronic, audio and visual. It applies to all council staff. 'Staff' for the purposes of this policy includes all council officers, volunteers and agency staff. While council contractors may be covered under their own terms and conditions, they are expected to adhere to council policies and procedures whilst handling information on behalf of the council.

3. Purpose

3.1. This policy represents the council's commitment to compliance with the accountability principle of data protection legislation and acts as the council's Appropriate Policy Document. Wyre Council will:

- Respect the rights of each individual;
- Ensure council processing of personal data is lawful and fulfils the appropriate general condition(s) for processing outlined in the UK GDPR (or Data Protection Act 2018 if acting as a 'competent authority' for 'law enforcement purposes') including any additional conditions set out in the Data Protection Act 2018 where special category data is being processed
- Be open and honest about the personal data it holds through the publication of overarching and service specific Privacy Notices;
- Provide training and support to those handling personal data in the course of their duties;
- Review and maintain Records of Processing Activities (RoPAs) on the personal data it processes either as Data Controller or Processor
- Adopt a stance of privacy by design and default including undertaking Data Protection Impact Assessments (DPIAs) where there may be a high risk to individuals' rights and freedoms

- Retain records only as long as required for business purposes
- Have appropriate organisational, technical, and security measures in place to protect personal data including maintaining logs of processing activities undertaken electronically
- Within required timescales inform the ICO and, in some instances, the data subject of any suspected or actual information security incidents where a high risk the rights and freedoms of affected individuals has been identified
- Have contracts or Information Sharing Agreements in place where personal data is regularly being shared with third parties
- Maintain our registration with the Information Commissioner's Office (ICO) (The council has two registration numbers Z5682712 (General Processing) and Z5682697 (Electoral Registration Officer)
- Appoint a Data Protection Officer (DPO)
- Create and maintain information management policies in addition to advising and issuing guidance to staff

4. Legal context

4.1. Reference to the following legislation and guidance may be required when reading this policy.

- The Data Protection Act 2018 (DPA 2018)
- The UK General Data Protection Regulations (UK GDPR)
- The Privacy and Electronic Communications Regulations (2003)
- The Freedom of Information Act 2000
- Regulation of Investigatory Powers Act 2000
- Computer Misuse Act 1990
- Human Rights Act 1998

4.2. Reference to the following internal council documents may also be required when reading this Policy;

- The council's Constitution
- Employee's Code of Conduct
- ICT Service Desk Computer Use Policy and User Agreement
- Information Security Policy
- Records Management Policy
- Password Policy and User Guidance

5. Roles and Responsibilities

5.1. Everyone representing the council has a duty to protect the information it holds and access to personal data must be on a strict need to know basis. Personal data must not be disclosed without appropriate authorisation. Failure to comply with data protection legislation could lead to serious consequences, and in some cases may result in significant fines or criminal prosecution

5.2. The council has an Information Governance Group which is accountable for ensuring compliance with this policy across the council. The group's primary membership consists of the Data Protection Officer and Deputy, representatives from ICT, Systems, and Transformation and is chaired by the Assistant Director of Governance and Legal (Monitoring Officer). The work of the group is supported by the Corporate Management Team and the Audit and Standards Committee. Updates are provided to the Senior Leadership Team quarterly

5.3. The council will ensure that:

- The DPO reports to the highest management level of the council in respect of their duties as DPO, in this instance, this is the Senior Information Risk Owner (Monitoring Officer) who forms part of the Senior Leadership Team.
- The DPO operates independently and is not dismissed or penalised for performing their task.

5.4. All data protection training provided by the council is mandatory and Line Managers are responsible for ensuring that all staff are given the necessary time to participate. Staff are required to participate in any mandatory 'bite size' exercises on cyber security and data protection training when instructed. The Information Governance team will provide guidance, advice, and support to anyone handling personal data as part of their role

6. Definitions

6.1. 'Personal data' under the UK GDPR means 'any information relating to an identified or identifiable natural person ('data subject')'

6.2. Special category personal data includes 'personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership' as well as the 'processing of genetic data, biometric data for the purposes of uniquely identifying a natural person' or data concerning physical or mental health, sex life or sexual orientation

6.3. 'Law enforcement purposes' are defined in the Data Protection Act 2018 as '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'.

6.4. Under the Data Protection Act 2018 'relevant personal data' means 'personal data contained in a judicial decision or in other documents relating to the investigation or proceedings which are created by or on behalf of a court or other judicial authority'.

6.5. 'Sensitive processing' is equivalent to the processing of special category personal data under the UK GDPR but also includes the processing of personal data as to the commission or alleged commission of an offence by an individual or proceedings for an offence committed or alleged to

have been committed, disposal of proceedings, or the sentence of a court. This is defined in the Data Protection Act 2018

7. Individuals' rights

7.1. Data protection legislation provides individuals with various rights. An individual's rights include:

- The right to be provided with specified information about the council's processing of their personal data **('the right to be informed').**
- The right to access their personal data and certain supplementary information **('the right of access').**
- The right to have their personal data rectified, if it is inaccurate or incomplete **('the right of rectification').**
- The right to have, in certain circumstances, their personal data deleted or removed **('the right of erasure', sometimes knowns as 'the right to be forgotten').**
- The right, in certain circumstances, to restrict the processing of their personal data **('the right to restrict processing').**
- The right, in certain circumstances, to move personal data the individual has provided to the council to another organisation **('the right of data portability').**
- The right, in certain circumstances, to object to the processing of their personal data and, potentially, require the council to stop processing that data **('the right to object').**
- The right, in relevant circumstances, to not be subject to decision-making based solely on automated processing **('Rights related to automated decision making, including profiling').**

7.2. In relation to the first right referred to above ('the right to be informed') in general the council will:

- where the personal data is collected from an individual, provide them with specified privacy notice information, at the time the personal data is collected, for example when a member of the public is signing up to receive a council service;
- where the personal data has not been obtained from an individual, provide them with specified privacy notice information within one month; if the council uses personal data that it has not collected directly from an individual to communicate with that individual, it

will provide the specified privacy notice information, at the latest, when the first communication takes place; if disclosure to another recipient of personal data, that has not been collected directly from the individual is envisaged, the council will provide the specified privacy notice information, at the latest, before the data is disclosed.

7.3. It should be noted that there are limited specified circumstances in which the right to be informed will not apply. For further information go to www.ICO.org.uk

7.4. Where an individual exercises one of the other rights listed above, the council will respond without undue delay and in any event within one calendar month, subject to the following two exceptions:

- Where further time is necessary, taking into account the complexity and the number of the request(s) from the data subject, the period for responding will be extended by up to two further calendar months. Where such an extension is required the council will notify the data subject that this is the case within one calendar month of receiving their request.
- Where the request(s) from a data subject are manifestly unfounded or excessive (in particular because of their repetitive character) the council will ordinarily refuse the request(s). In exceptional cases the council may instead exercise its alternative right in such circumstances to charge a reasonable fee that takes into account the administrative cost of complying with the request.

7.5. The council recognises the fundamental nature of the individual rights provided by data protection legislation. The council will ensure that all valid requests from individuals to exercise those rights are dealt with as quickly as possible and by no later than the timescales allowed in the legislation.

7.6. To minimise delays, and to help ensure that the council properly understands the request being made, it is preferable for requests from data subjects wishing to exercise their data subject rights to be either in writing or made via the council's on-line process. However, a valid request may also be made verbally.

7.7. The council's dedicated email address for exercising individual rights is informationgovernance@wyre.gov.uk or individuals can use the council's online form available from the council's website at; https://www.wyre.gov.uk/info/200373/your_data_and_us

7.8. All requests from data subjects to exercise their data subject rights will be handled in line with the Subject Access Protocol

7.9. Data protection law allows exemptions from complying with data subject rights in specific and limited circumstances. The council will normally

apply the exemptions where they are engaged, unless it is satisfied that it is appropriate or reasonable not to do so.

7.10. If a data subject exercising one or more of their data subject rights is dissatisfied with the response received from the council, they may make a complaint to the council's Data Protection Officer (DPO) in the first instance.

8. Individuals' Rights – Law Enforcement Processing

8.1. The rules relating to an individual's rights are different where the council processes personal data as a 'competent authority' for 'law enforcement purposes'. In those circumstances individuals have the following rights:

- the right to be informed;
- the right of access;
- the right to rectification;
- the right to erasure or restriction of processing; and
- the right not to be subject to automated processing.

8.2. There are no equivalents to the right to object or the right to data portability. Also, the right of access, the right to rectification and the right to erasure or restriction of processing will not apply to 'relevant personal data' in the course of a criminal investigation or criminal proceedings.

8.3. Where an individual exercises their rights in respect of personal data that the council is processing for law enforcement purposes the council will ordinarily respond without undue delay and in any event within one calendar month. There is not an option for the council to extend this for a further period in the case of complex or numerous requests, although the council can refuse (or make an administrative charge for) manifestly unfounded or excessive requests.

9. Data Protection principles

9.1. The council will comply with the principles relating to the processing of personal data set out in the UK GDPR by putting in place processes 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 for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial 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; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (accuracy);

- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; (personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the UK GDPR in order to safeguard the rights and freedoms of the data subject) (storage limitation) and;

- 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)

9.2. The council shall be responsible for, and be able to demonstrate compliance with, all the above principles (accountability).

9.3. Where the council processes personal data as a 'competent authority' for 'law enforcement purposes' (i.e. under statutory law enforcement functions) it shall do so in accordance with the version of the data protection principles set out in the Law Enforcement provisions of the DPA 2018. Those principles are similar (but not identical) to the principles applying to more general processing of personal data detailed above.

10. Compliance with Principle a: lawfulness, fairness, transparency

10.1. The council processes personal data mostly frequently to fulfil its statutory obligations, exercising its discretionary powers or otherwise acting in the public interest. The council also processes personal data in its role as an employer but may also rely on other lawful bases depending on the activity being undertaken. These are specified in the individual service Privacy Notices

10.2. As part of our statutory and corporate functions, we process special category and criminal offence data under:

- UK GDPR Article 6(a): consent to processing for one or more specific purposes

- UK GDPR Article 6(b): 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
- UK GDPR Article 6(c): legal obligation to which Wyre Council is subject
- UK GDPR Article 6(d): protection of vital interests of data subject or other natural person
- UK GDPR Article 6(e): performance of a task carried out in the public interest or in the exercise of official authority vested in Wyre Council
- UK GDPR Article 6(f): legitimate interests of Wyre Council or a third party

10.3. Wyre Council processes special category data under:

- UK GDPR Article 9(2)(a): explicit consent for one or more specified purposes
- UK GDPR Article 9(2)(b): carrying out the obligations and exercising specific rights of the council or the data subject in the field of employment and social security and social protection law as authorised by domestic law. Our basis for processing this special category data may be found in the Data Protection Act 2018 Schedule 1, Part 1, section 1: employment, social security and social protection
- UK GDPR Article 9(2)(c): protection of vital interests of data subject or other natural person where consent cannot be given
- UK GDPR Article 9(2)(f): establishment, exercise or defence of legal claims
- UK GDPR Article 9(2)(g): reasons of substantial public interest on the basis of domestic law. We rely on the following Substantial Public Interest Conditions listed in Schedule 1, Part 2 of the Data Protection Act 2018:

  (6) Statutory and government purposes
  (11) Protecting the public against dishonesty
  (18) Safeguarding of children and of individuals at risk
  (24) Disclosure to elected representatives

- UK GDPR Article 9(2)(h): preventative or occupational medicine, assessment of the working capacity of an employee, medical diagnosis, provision of health or social care or treatment or management of health of social care systems and services on the basis of domestic law or pursuant to contract with a health professional. Our basis for processing this special category data may

be found in the Data Protection Act 2018 Schedule 1, Part 1, section 2: health or social care purposes

- UK GDPR Article 9(2)(i): public health on the basis of domestic law. Our basis for processing this special category data may be found in the Data Protection Act 2018 Schedule 1, Part 1, section 3: public health

10.4. While not formally defined as a 'special category' of personal data under the UK GDPR, similar additional conditions and requirements also apply to personal data relating to criminal convictions and offences (including personal data relating to the alleged commission of offences and proceedings relating to the commission or alleged commission of offences). The council processes criminal offence data under the control of its official authority as specified in Article 10(1) of the UK GDPR

10.5. Where the council processes personal data as a 'competent authority' for 'law enforcement purposes' it shall do so in accordance with the requirements of the law enforcement provisions of the DPA 2018. In all cases such processing will only be carried out where the individual concerned has given their consent to the processing of their personal data for law enforcement purposes or where the processing is necessary for the performance of a task carried out for law enforcement purposes by a competent authority. Where such processing involves 'sensitive processing' the council will ensure that the processing is strictly necessary and (unless the individual has consented to the processing) that one of the conditions for sensitive processing set out in the DPA 2018 is met.

10.6. Fair: The council's commitment to this principle is underpinned by the principles of privacy by design and privacy by default. 'Privacy by design' means that the council will take into account privacy issues from the very outset of planning for an activity that might involve the processing of personal data. 'Privacy by default' means that the council will ensure that only personal data that is necessary for a specific purpose is processed. The council will not collect more personal data than is needed for the purposes concerned, process it more than is necessary or store it longer than is needed.

10.7. The council will follow relevant guidance issued by the Government, the ICO, and the Surveillance Camera Commissioner for users of CCTV and similar surveillance equipment monitoring spaces to which the public, residents, service users and staff have access.

10.8. When we share personal or special category data or criminal offence data with another controller, processor or jurisdiction, we will ensure that contracts and data sharing agreements are in place and are compliant with relevant laws and regulations.

10.9. Transparent: The council has an overarching privacy notice and service specific Privacy Notices that can be found on the council's website. Alongside this Data Protection Policy, the council also maintains a Records Management Policy and an Information Security Policy.

11. Compliance with Principle (b): purpose limitation

11.1. The council processes personal data for specific purpose(s) including for law enforcement purposes. The council maintains Records of Processing Activities (RoPAs) which detail its processing activities and provides the majority of this information online in its service specific Privacy Notices

11.2. Personal data may be shared across council departments and with contractors working on the council's behalf for legitimate purposes, such as:

- Updating council records;
- Providing services; and
- Preventing and detecting fraud.

11.3. The council does not process personal data for purposes that are incompatible with the purposes for which it was collected. Where it is proposed to use council data outside its original purpose, we will conduct a compatibility assessment excepting a legal obligation compelling us to comply

11.4. The council may also, in appropriate circumstances, make discretionary disclosures of personal data to a person or organisation other than the data subject where it is permitted to do so by law. When deciding whether to exercise its discretion to disclose personal data in such circumstances the council will always give proper consideration to the data subject's interests and their right to privacy.

12. Compliance with Principle (c): data minimisation

12.1. We collect personal data necessary for the relevant purposes specified in our service specific Privacy Notices. This information is adequate and proportionate to our purposes. We will pseudonymise personal data where appropriate

12.2. Preliminary Data Protection Impact Assessments (DPIAs) have been embedded into the council's project planning documentation and are passed to the Information Governance team for review. Full DPIAs are completed where processing is on a large scale or there is a high risk to the rights and freedoms of those individuals whose data is being processed

12.3. We do not systematically collect or harvest sensitive personal data for law enforcement purposes. The information we process is necessary for and proportionate to our purposes and processed to meet these purposes.

13. Compliance with Principle (d): accuracy

13.1. Where we become aware that personal data is inaccurate or out of date, having regard to the purpose for which it is being processed, we will take every reasonable step to ensure that data is erased or rectified without delay. If we decide not to either erase or rectify it, for example because the lawful basis we rely on to process the data means these rights do not apply, we will document our decision

14. Compliance with Principle e: storage limitation (Records Management)

14.1. The council manages and disposes of its records in accordance with the council's Records Management Policy and retention schedules so that records are not retained longer than required. Different types of information may be held for different lengths of time depending on legal and operational requirements. Once the retention period has passed, personal data will be disposed securely unless a need for further retention has been identified and documented

15. Compliance with Principle f: integrity and confidentiality (Information Security)

15.1. Effective methods of security are in place to help prevent the inappropriate disclosure or loss of personal data including appropriate access controls. Full details of the council's commitment to this principle may be found in the Information Security and Handling Policy

15.2. Our ICT systems maintain logs of processing activities undertaken electronically recording as a minimum the user ID, date, and action taken

15.3. In the event of a suspected data breach, staff must follow the guidance for reporting potential breaches detailed on the HUB to ensure timely reporting to the ICO in case of a serious incident which may present a high risk to the rights and freedoms of the affected data subjects

16. Governance and Distribution

16.1. The ownership of this policy sits with the Information Governance Group (IGG) who will ensure it remains consistent and compliant with the law, and any advice and codes of practice issued from time to time by the ICO. The group will review the policy annually with any changes being submitted to the Audit and Standards Committee for approval.

16.2. The policy will be displayed on the council's Hub and also the council's website on the data protection web page:

https://www.wyre.gov.uk/info/200373/your_data_and_us

Appendix A Sources of information and guidance

This policy is supported by training, awareness and additional guidance made available to staff on the council's Hub. The ICO also provides a free helpdesk that can be used by anyone and a website containing a large range of resources and guidance on all aspects of information law for use by organisations and the public. Please see www.ico.org.uk

Other useful contact details

Data Protection Officer	01253 887428
Deputy Data Protection Officer	01253 887233
ICT Service Desk	01253 887652
Information Commission Officer helpline	0303 123 1113