| Title: | Data Assurance Policy |
|---|---|

## Section 1: Introduction

1.1 Good quality information supports good quality decision-making. So good quality information is essential to Fylde Council. This policy sets out (in section 3) how the council ensures the quality of the information that it uses.

1.2 The council does not have a free hand in deciding what it does with the information that it keeps and uses. Under the Freedom of Information Act 2000, there is a presumption that all of the information held by the council should be available to the public on request. The council can only refuse a request for information in certain circumstances set out in the act. Conversely, under the Data Protection Act 2018, the council can only process personal data in accordance with that act.

1.3 This policy therefore also describes (in section 4) how the council complies with its obligations under the Data Protection Act to properly protect the information that it holds and (in section 5) the steps it has taken to make it easier to know how particular items of information should be dealt with.

1.4 This policy applies to all staff. As a matter of good practice, agencies and individuals working with the Council, and who either provide or have access to information held by the council will be expected to have read this policy and comply with those parts that apply to them. External entities can only be given access to personal information held by the council if the Data Protection Act allows it. Usually this will mean that there needs to be a written contract term or data sharing agreement.

## Section 2: Definitions

**Personal Data**

Any information relating to a living individual who can be identified from that information or from that data and other information in possession of the data controller. This includes expression of opinion about the individual, and of the intentions of the data controller in respect of that individual.

**Special Category Data**

Personal data that relates to racial or ethnic origin, political opinions, religious or

philosophical beliefs, trade union membership, genetic data, health, sex life, sexual orientation or criminal convictions[1]. Special category data is subject to much stricter conditions of processing.

**Data Controller**

Any person (or organisation) who makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data is processed and the way in which it is processed. The Council is the data controller for the purposes of this policy

**Data Subject**

A person who is the subject of personal data.

**Processing**

Virtually anything that can be done to data, including accessing, altering and destroying it.

**Processor**

A person or organisation which processes personal data on behalf of a controller

**Third Party**

Any individual/organisation other than the data subject, the data controller (the Council) or its agents.

## Section 3: Data Quality

3.1 Every employee has a responsibility for information quality whenever they record, use or publish information. Directors have an overall responsibility for making sure that their directorate has appropriate practices and procedures for ensuring the quality of information recorded, used or published by their directorate. Recording information includes making a record of it on paper, electronically or by any other media. Using information includes making decisions based on it, or presenting it (for example, as part of a report) to somebody else. Publishing it means making it available to the public or a section of the public.

3.2 Good quality information is **accurate**, **available** and **useful**.

**Accurate:**

3.3 If the information is factual, it should be true insofar as the person recording it and the person using it can reasonably ascertain. If the information is opinion, it should represent the true and reasonable view of the person providing it and should be identifiable as opinion in the context it is used.

3.4 There should be enough information for the purpose, but not too much. Incomplete information can sometimes be misleading. But presenting too much information can lead to confusion.

**Available:**

[1] Information about criminal convictions is protected separately from special category data by legislation but is considered alongside it for the purposes of this policy.

3.5 If information is not available, it should not be kept. Information is only available if it is both physically accessible and searchable.

3.6 Information is searchable if there is some system for finding it and (where appropriate) finding out what is in it. This need not be electronic, and could include manual catalogues or indexes. But it should not be left to the memory of individuals, as individuals can forget or leave the council.

3.7 Information is only available if someone has not taken it away. So there should be appropriate processes to ensure the security of information. These will vary depending on the information involved. However, there are specific legal requirements about security of personal data. These are dealt with in more detail under section 4 (data protection).

**Useful:**

3.8 Information is only useful if it is up-to-date for the purposes for which it is to be used and can be understood.

3.9 Modern technology makes it easier to access up-to date information and less necessary to keep a local copy of it. For example, it will almost never be necessary to keep a paper copy of a document that is available online. Information should always be checked for accuracy before it is published or used.

3.10 Information that cannot be understood by its audience is not useful. Highly technical information should be summarised or accompanied by an explanation if it is intended for a lay audience.

## Section 4: Data Protection

4.1 The Council is committed to protecting the rights and privacy of individuals (including customers, staff and others) in accordance with the Data Protection Act. The Council needs to process certain information about its staff, customers and other individuals it has dealings with for administrative purposes (e.g. to recruit and pay staff, to carry out its functions, and to comply with legal obligations). To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed unlawfully.

4.2 This part of the policy sets out what you need to do to help the council comply with its legal obligations. It does not repeat the whole of the law about data protection. You can get advice that is more detailed from the Head of Governance, who is the Council's statutory data protection officer.

4.3 The Council is registered with the Information Commissioner as a body that holds personal data. The Head of Governance keeps the Council's registration up to date. Details of the Council's registration are published on the Information Commissioner's website.

**Data Protection Principles**

4.4 You must only process personal data in accordance with the eight data protection principles. These are contained in the Data Protection Act and summarised here:

1. ***Lawfulness, fairness and transparency.***
   *You must have a lawful basis for processing the data and ensure that you do not do anything with it that is in breach of any other laws. You must not process the data in a way that is unduly detrimental, unexpected or misleading to the individuals concerned and you must be clear, open and honest about how you will use the data. (see further the section on privacy notices).*
2. ***Purpose limitation.***
   *You must be clear about what your purposes for processing are, record them and specify them in your privacy information for individuals.*
3. ***Data minimisation.***
   *You must ensure the data is adequate, relevant and limited to what is necessary for your purpose.*
4. ***Accuracy.***
   *You should take all reasonable steps to ensure the data is factually correct, and you should keep it updated where appropriate. You should promptly correct any inaccurate or misleading data and consider any challenge about its accuracy.*
5. ***Storage limitation.*** *(see the section on Retention and Disposal of Data)*
6. ***Personal data shall be processed in accordance with the rights of data subjects under the Data Protection Act.*** *(see the section on Data Subjects' Rights)*
7. ***Integrity and confidentiality.*** *(see the section on Security of Data)*
8. ***Accountability.***
   *You to take responsibility for what you do with personal data and how you comply with the other principles. You must have appropriate measures and records in place to be able to demonstrate your compliance.*

**Privacy notices**

4.5 When you collect personal data from someone, you must give them information including: the council's purposes for processing their personal data, how long we will keep it, and who it will be shared with.

4.6 When you obtain the data from somebody else, you must give the data subject the privacy information no later than one month after obtaining it.

4.7 There are a few circumstances when you do not need to provide people with privacy information, such as if an individual already has the information or if it would involve a disproportionate effort to provide it to them.

4.8 The information you provide to people must be concise, transparent, intelligible, easily accessible, and it must use clear and plain language.

4.9 There are examples of privacy notices you can adapt on the intranet.

**Data Subject Rights**

4.10 Data Subjects have the following rights concerning personal data about them:

- To be informed about the collection and use of their data.
- To access their data.
- To have inaccurate data rectified, or completed if it is incomplete.
- In certain circumstances, the have the data erased.
- In certain circumstances, to restrict or suppress their data.
- to obtain and reuse data they have provided for their own purposes across different services.
- In certain circumstances, to object to the processing of their data.
- To obtain information about automatic decision-making using their data and to request human intervention in the process.

**Lawful basis for processing personal data**

4.11 The Council can generally only collect use or disclose data if one of the conditions summarised in this section applies:

- The data subject has given their genuine consent
- It is necessary in connection with a contract with the data subject
- comply with a legal obligation (except a contract)
- It is necessary to protect the vital interests of the data subject: that is, a medical emergency
- It is necessary so that the Council can carry out a function or perform a specific task in the public interest that is set out in law

4.12 If you are in any doubt about whether data can be processed in a particular way, get advice from your manager or the Data Protection Officer.

**Security of Data**

4.13 You must make sure that any personal data which you deal with is kept securely and is not disclosed to any unauthorised third party (see the section on Disclosure of Data for more detail).

4.14 All personal data should be accessible only to those who need to use it. You should form a judgement based upon the nature of the information in question, but always consider keeping hard copy personal data:

- in a lockable room with controlled access, or
- in a locked drawer or filing cabinet

4.15 Don't keep personal data on a local hard drive, a laptop or removable media. Only keep it on the council's network drives , or within a third party application that can be

accessed from the network drives. Don't keep personal data in any shared folders, unless they are password protected.

4.16 Take care that PCs and laptops are not visible except to authorised staff and that computer passwords are kept confidential. Do not leave PC screens unattended without password protected screen-savers. Don't leave manual records where they can be seen by unauthorised personnel.

4.17 Put appropriate security measures are in place for deleting or disposing of personal data. Shred manual records or dispose of them as "confidential waste". Wipe clean or destroy hard drives of redundant PCs before disposal.

4.18 This policy also applies to processing of personal data "off-site". Off-site processing presents a potentially greater risk of loss, theft or damage to personal data. Take particular care when processing personal data at home or in other locations outside the Council's offices. Personal data should only be loaded to removeable media after discussion with the Data Protection Officer.

4.19 Do not store personal data belonging to the council in a cloud-based storage facility without the specific consent of your Head of Service, who should consult with the council's IT section.

**Rights of Access to Data**

4.20 Data subjects can request access any personal data about which the Council holds about them. If you receive a request, you should ask for it to be put in writing and either:

- refer the request to the Data Protection Officer, or
- if the request is specific to information that you control, disclose it (but only after making sure that the person requesting it is the data subject)

4.21 Any such request must be complied with within a month of receipt of the written request. There are some exemptions to the right to access personal data. If you feel that an exemption may apply, contact the Data Protection Officer.

4.22 You must also give the following information to anyone who makes a request to access their data:

- the purposes of processing;
- the categories of data concerned;
- the recipients or categories of recipient the council disclose the data to;
- the retention period for storing the data, or how we will determine how long you will store it;
- the existence of the  to request rectification, erasure or restriction or to object to processing;
- the right to lodge a complaint with the Information Commisioner;
- where we got the data, if it was not obtained directly from the individual;
- the existence of automated decision-making (including profiling); and
- the safeguards the council provides if it transfers personal data to a third country or international organisation.

4.23 The right to request access applies to any personal data held about a person. However, if the data is not kept or ordered by reference to individuals, the data subject would normally have to say what data they wish to see. The Council could refuse the request if complying with it exceeds a cost limit set by government.

**Disclosure of Data**

4.24 The Council must ensure that personal data is not disclosed to unauthorised third parties, which include family members, friends, government bodies, and in certain circumstances, the Police. You should exercise caution when asked to disclose personal data held on another individual to a third party. For instance, it would usually be appropriate to disclose a colleague's work contact details in response to an enquiry regarding a particular function for which they are responsible. However, it would not usually be appropriate to disclose a colleague's work details to someone who wished to contact them regarding a non-work related matter. Nor would it be appropriate to give home contact information. The important thing to bear in mind is whether or not disclosure of the information is relevant to, and necessary for, the conduct of Council business. Best practice, however, would be to take the contact details of the person making the enquiry and pass them onto the member of staff concerned.

4.25 As well as the conditions listed in 4.6, there are some other specific instances where disclosure to a third party is allowed. These concern national security, crime and taxation and regulatory activity. If any issue arises about these, or if in doubt, ask for advice from your manager or the Data Protection Officer.

4.26 There are some other exemptions not listed here which would be unlikely ever to arise.

**Retention and Disposal of Data**

4.27 The council has a separate policy on data retention, based upon guidance and classifications provided by the Information and Records Management Society.

## Section 5: Data classification

5.1 The council has adopted a simple classification system to make it easier to identify how information that it holds should be treated. The system is intended to reflect the statutory position under the Data Protection Act 2018 and the Freedom of Information Act 1990. The council considers that any advantages of introducing a more complex system of classification would be outweighed by the burden of implementing such a system.

5.2 The classifications are:

- **Personal Information**: This is information that is personal data or special category data as defined under the Data Protection Act 2018. In other words, it is information that the council cannot (except with the consent of the data subject or in certain other limited circumstances) disclose
- **Excluded Information**: This is information that, on an application for disclosure under the Freedom of Information Act 2000, would be likely to be withheld from

disclosure under any of the exemptions other than the exemption applicable to personal data. In other words, it is information that the council may, but need not, disclose.

- **Unrestricted Information**: This is information that, on an application under the Freedom of Information Act 2000, the council would be obliged to disclose.

5.3 From the implementation of this policy, employees will be encouraged to discreetly mark Personal and Excluded Information so that users of that information will be alerted to its status. Unrestricted Information may also be marked as such. Marking an item of information as Personal, Excluded or Unrestricted will not be conclusive of its status. An employee using any information must always consider the principles set out in this policy, as well as the requirements of the Data Protection Act 2018.

5.4 Where an item is marked as Excluded Information, it must not normally be published or disclosed without first giving full consideration to how the council's interests (or the interests of any other person who might be affected by the publication or disclosure) might be affected if it was published or disclosed.

5.5 Where an item is marked as Personal Information, it must not be published or disclosed (except to the data subject) without the approval of the relevant head of service.

## Section 6: Monitoring and Review

6.1 The council's Management Team will monitor and keep this policy under review. They will judge its success by the following criteria:

- The quality of information available to decision-makers
- Compliance with the council's obligations as data controller under the Data Protection Act 2018
- The balance between the advantages secured by the policy and the burdens imposed by it.