##### Elected Member Data Protection Policy – general, special category, and crime personal data

**Version 1**

May 2019

1. **Objectives**
	1. This policy sets out the key data protection obligations and accountability to which we are fully committed. This policy applies to general personal data processing together with special category and criminal convictions and offence data. It explains how the data protection principles are met and provides an indication of how long such personal data is likely to be retained.
2. **Scope**
	1. As Elected Members we need to collect, use, receive and share personal, special personal and crime personal data about living people
	2. This policy covers all aspects of handling personal data, regardless of age, format, systems and processes purchased, developed and managed by/or on behalf of us and any person directly employed or otherwise by us.
	3. This policy reflects the commitment to data protection compliance to both UK and EU legislation, the Data Protection Act 2018, the EU General Data Protection Regulation 2016 (GDPR)
3. **Policy**
	1. Definitions of personal data:

***Personal data*** *means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, 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;*

In summary, anything and everything that can relate to a living person.

**Special Personal data** means *personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*

In summary, these are the data categories that are subject to additional controls in order to prevent unauthorised collection, use, access etc.

**Crime data** means criminal offence data, e.g., alleged commission of offences or proceedings for an offence, (actual or alleged), including sentencing

In summary this type of personal data is subject to specific conditions and controls.

* 1. Data Protection Principles: There are 6 principles which provide the framework for personal data handling.

Personal data shall be:

1. *processed lawfully, fairly and in a transparent manner*

To be lawful an appropriate condition of processing needs to be identified. To be fair and transparent a privacy notices needs to be provided/available to the data subject whose personal data is being handled (data subject) and the law specifies what information must be communicated.

1. *processed for an explicit and specific purpose and not processed for other incompatible purposes. Scientific/historical/statistical research is not incompatible and nor is archiving in the public interest*

Personal data should only be used other than for the stated lawful purposes, except where the law permits.

1. *adequate, relevant and limited to what is necessary for the purpose*

Ensure that personal data is specific to the stated lawful purpose and is not excessive or unnecessary.

1. *accurate and, where necessary, kept up to date; ensuring that personal data that are inaccurate, are erased or rectified without delay*

Ensure that personal data is correct and that any errors are rectified and where appropriate notified to recipients of the personal data.

1. *keep no longer than necessary for the purpose, but can keep for longer is solely for Scientific/historical/statistical research and archiving in the public interest purposes and is kept securely*

Personal data should not be kept longer than necessary taking into account legal and operational requirements.

 *(f) protection of the personal data using appropriate technical or organisational measures*

These measures should be selected on the basis of identified threats and risks to personal data and the potential impact on the data subjects, we and any third parties who are sources, recipients, or processors of the personal data.

* 1. Data Collection, use and disclosure: We handle personal data that has been either collected from the data subject and/or other parties, e.g. other people, public sector and regulatory organisations, private and voluntary sector organisations etc.

3.3.1 As Elected Members we will:

* only handle personal data where there is a legal basis to do so and provide data subjects with privacy notices that explain why the personal data is required and how to exercise their personal data rights.

In summary processing personal data in connection with issues raised by constituents, involving constituents and other people with whom liaison is required, eg, sharing/disclosing information as required,in order to pursue or resolve the issues raised. <https://www.oldham.gov.uk/downloads/file/5238/privacy_notice_-_councillors>

* Maintain a record of processing activities (ROPA) in accordance with the law.

<https://www.oldham.gov.uk/downloads/download/1390/ropa_records_of_processing_activities>

* Avoid holding any personal data beyond what is necessary and ensure personal data is subject to appropriate retention and security controls taking into account the nature of the data and the information risks. Personal data may be stored for longer periods where it is for archiving in the public interest, historical or scientific research purposes, or as required by legislation or regulatory activity.
* where it is appropriate to do so, take reasonable steps to check that information provided is accurate, and where any inaccuracies are discovered, these are promptly corrected and any third party recipients of the innacurate data notified of the correction.
* Hold personal data on devices, software, networks that suitably protected from unauthorised access.
* in the event of a personal data security breach, resulting in a high risk to the data subject(s), to notify the data subjects and / or the ICO as appropriate.
* in the event of a data subject exercising their personal data rights, we will assess the request and respond within the statutory timeline and provide a complaints process.
* not transfer personal data outside of the European Economic Area (EAA) to countries with lower data protection standards, unless the appropriate safeguards and controls are in place
* to co-operate and provide information to the ICO and other regulatory bodies in pursuance of any investigation or enforcement action.

3.4 Offences: The data protection legislation contains specific offences:

3.4.1 It is an offence for a person knowingly or recklessly, without the consent of the data controller, to

* obtain or disclose personal data
* procure the disclosure of personal data to another person
* retain it without the consent of the original data controller
* offer to sell or buy the personal data obtained

.

3.4.2 It is an offence for a person knowingly or recklessly to re-identify information that is de-identified personal data without the consent of the controller, or to knowingly or recklessly handle such data.

3.4.3 It is an offence to alter, deface, block, erase, destroy or conceal information with the intention of preventing disclosure of all or part of the information that the data subject making the request for access or portability would have been entitled to receive.

3.4.4 It is an offence to require a data subject to provide or give access to information obtained via data subject access in relation to health, conviction/caution records for the purpose of recruitment, continued employment, in connection with provision of goods and service to the public. In summary a data subject should not be obliged to make a data subject access request for this type of information as a condition/implied condition of employment or contract.

3.4.5 It is an offence to intentionally obstruct or give false information to the ICO in the exercise of its powers under information notices and/or warrants.