

Handling Oldham Council Information Policy

**Version: 5.0**

**Dated: February 2023**

**Status: Final**

**Document Control**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version / Issue No.** | **Date** | **Author** | **Purpose/Changes** |
| V0.1 | July 2014 | Stephen Hankinson |  |
| V0.2 | September 2014 | Stephen Hankinson | Review |
| V0.3 | November 2014 | Stephen Hankinson | Review |
| V0.4 | February 2015 | Stephen Hankinson | For sign off |
| V1.0 | February 2015 | Stephen Hankinson | Approved |
| V1.1 | May 2018 | Nadeer Hussain | Review in lieu of Data Protection Legislation / General Data Protection Regulations |
| V2.0 | May 2018 | Nadeer Hussain | Final |
| V3.0 | May 2019 | Nadeer Hussain | Annual Review |
| V3.1 | November 2019 | Nadeer Hussain | Update in lieu of Data Protection Legislation / General Data Protection Regulations |
| V3.2 | November 2020 | Nadeer Hussain | Review |
| V4.0 | December 2020 | Nadeer Hussain | Final |
| V5.0 | February 2023 | Nadeer Hussain | Final |

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 24 months.

**Contents**

1 Introduction

2 Information Assets

3 Classification of Personal Information

4 Cyber Security

5 Sharing Information

6 Suppliers / Contractors / Sub-Contractors

7 Authority for this Policy

Appendix 1

Appendix 2

Appendix 3

**1 Introduction**

Information is a key asset that, like other important business assets, has value to Oldham council and consequently needs to be suitably protected. We have a responsibility and requirement to protect its information.

This policy

* ensures information is protected to ensure that high confidentiality, integrity, availability and resilience standards of information are maintained
* clarifies guidance on handling rules for Oldham council information, including personal data, Special category data, Crime data and information which originates from the Public Services Network (PSN), i.e. information supplied to us by central government, health, or occasionally other Local Authorities
* meets the requirements of relevant legislation and in particular relates to elements of Principle f of the General Data Protection Regulation (GDPR). Readers should however, remember the importance and necessity of compliance with all 6 Principles of GDPR and the Data Protection Act 2018 – Appendix 1 refers
* in addition, for those working in health and social care there is an obligation to follow the Caldicott Principles, National Data Guardian Standards (Appendix 3) and the law of confidentiality.
* applies to all information that Oldham council collects, stores, processes, generates or shares to deliver services and conduct business, including information received from or exchanges with external partners

Owing to the potential for harm and distress from compromise, the impact on reputation and the potential for enforcement or regulatory action and / or monetary penalties, the protective measures required for use, storage, transfer, sharing of personal information, particularly when aggregated, are more stringent than for non-personal data.

In accordance with Part 6 of the Data Protection Act 2018, the maximum penalty that may be imposed is;

* the amount specified in Article 83 of the GDPR;
* the “higher maximum amount”: which is in the case of an undertaking, the higher of 20,000,000 EUR or 4% of the undertaking’s total annual worldwide turnover in the preceding financial year, or in any other case 20,000,000 EUR; or
* the “standard maximum amount”: which is in the case of an undertaking the higher of 10,000,000 EUR or 2% of the undertaking’s total annual worldwide turnover in the preceding financial year, or in any other case 10,000,000 EUR.

Non-compliance with this policy could have a significant effect on the efficient operation of the council and may result in financial loss, fines, and / or an inability to provide necessary services to our customers.

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

* obtain or disclose personal data
* procure the disclosure of personal data to another person
* retain it without the consent of Oldham council
* offer to sell or buy the personal data obtained
* re-identify information that is de-identified personal data
* 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

This policy applies automatically to the systems, people and business processes comprising the council’s information systems. This includes (but may not be limited to) all Oldham council Elected Members, committees, departments, partners, employees of the council, contractors, agency staff, voluntary agencies of the council that require access to council information systems; or information of any type or format, e.g. paper or electronic.

If you do not understand the implications of this policy or how it may apply to you, you must seek advice.

If your action (or inaction) causes a breach of this policy, you may be liable for the cost of resolving any issues or be liable for any fines relating to the loss of the information.

**Suppliers of goods and services to the council are directly responsible for cascading this policy to their staff.**

The term “council information” covers all information for which the council is the information asset owner – this is not limited to personal information (PII) but also includes any information which is not known to the public (business sensitive).

Oldham council is responsible for the information it holds, whether it is personal data, business information or information held on behalf of a third party. The council has a responsibility to ensure that there are no breaches in relation to:

* Security
* Data Protection Act 2018 / GDPR
* Human Rights
* Confidentiality
* Freedom of Information
* Intellectual Property
* Copyright
* Regulation of Investigatory Powers Act
* Lawful Business Practice Regulations
* Other related legislation
* Standards of practice and conduct

**2 Information Assets**

The process of identifying important information assets should be sensible and pragmatic.

Important information assets will include, but are not limited to, the following:

* Paper records
* Computer databases
* Information files and folders

It is important to inventory significant information assets that are relied on. Such an inventory identifies each asset and all associated information required for risk assessment, information / records management and disaster recovery. Such inventories include the following:

* Type
* Location
* Designated owner
* Security classification
* Format
* Backup
* Licensing information

All important information assets must have a nominated owner and should be accounted for. An information asset owner must be someone whose seniority is appropriate for the value of the information asset they own. The owner’s responsibility for the asset and the requirement for them to maintain it should be formalised and agreed. Items of information that are of limited or no practical value do not automatically require a formal owner or listing on inventories.

Information should be destroyed if there is no legal or operational need to keep it and this must be done in way that is commensurate to the type of information, e.g. personal sensitive information on a computer hard drive should be securely wiped in line with ISO 27001 and the National Cyber Security Centre (NCSC) guidelines. Special category data or Crime data in a paper record should be cross shredded before disposal.

**3 Classification of Personal Information**

On creation, all personal information must be assessed and classified by the information asset owner according to their content.

The categorisation should indicate the sensitivity of the information in terms of likely impact resulting from compromise, loss or misuse. The categorisation will determine how documents and information should be protected and who should be allowed access to them.

Oldham council personal information may be categorised into five types:

* Personal Data
* Special category data
* Crime data
* Personal data for EU Law Enforcement Directive 2016 (LED) purposes
* Personal information originating from the PSN network – see detail below

Each attracts a baseline set of information protection / security controls providing appropriate protection against typical threats. Additionally, ICT systems and services may require enhanced controls to manage the associated risks to aggregated information or to manage confidentiality, integrity and availability concerns.

**Personal Data**

As defined by GDPR, 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.

Examples of personal data include:

* Name
* Postal address – business / home
* Email address
* Telephone / mobile number
* Driving License Number
* Date of birth
* National Insurance Number
* Financial Information
* IP address

**Special Category Data**

This type of data could have more damaging consequences for individuals or the council if it were lost, stolen or published in the media. Special category data as defined by GDPR 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.

Examples of Special category data within the council include:

* Benefit or pension records
* Health records
* Care orders
* Child protection records
* Adoption records
* Educational records
* Ethnicity
* Fingerprint

**Crime data**

Crime data as defined by GDPR means criminal offence data, e.g., alleged commission of offences or proceedings for an offence, (actual or alleged), including sentencing, where it is NOT USED for the purposes of the prevention, investigation, detection or prosecution of criminal offences, the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. In summary this type of personal data is subject to specific conditions and controls.

**Personal data for LED purposes**

Means the handling of personal data for the purposes the prevention, investigation, detection or prosecution of criminal offences, the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. In summary personal data used for this purpose is subject to specific data protection conditions and controls.

**Information Originating from the PSN Network**

Information originating from the PSN is information supplied to us by central government, health, or occasionally other Local Authorities. The council is required as a part of its compliance with being connected to the PSN, to honour the controls requested in relation to the information provided through this network. Some of these controls are in relation to the council’s ICT Infrastructure. Other controls are in relation to Information Management and Governance.

The controls that apply to all information originating from PSN must be adhered to unless an authorised originating Data Controller provides alternative written advice.

When assessing the information and use of information from a PSN source, it is important to be pragmatic. For instance:

* A database of names and addresses that is a replication of information the council already creates and stores itself ought to be handled as council Personal Data
* Information provided via PSN that would also be publicly accessible would not necessarily require the same level of controls as dictated by the overarching PSN requirements

Personal, Special category, Crime or information originated from PSN could have more damaging consequences for individuals or the council if it were lost, stolen or published in the media.

Bulk data stores make very tempting targets for attackers of all kinds and it is therefore essential to ensure they are adequately protected.

The NCSC is a recognised UK Government technical authority on cyber threats and exists to bridge industry and government together by providing support, advice and guidance on cyber security. It is important you are aware of guidance provided by the NCSC and have steps and measures in place to ensure you follow recommended standards The NCSC has provided good practice measures which provides a set of indicators against which the security of information assets can be objectively appraised.

This is not a definitive set of measures. The list managed by the NCSC will necessarily change over time, as the attacks and techniques used by adversaries change. It is therefore important that good practice measures are not seen as an alternative to a risk management strategy designed to protect bulk personal data.

To assist the council in protecting information in line with the Data Protection act, the council expects all Suppliers / Contractors acting on behalf of the council to follow at a minimum the following guidance;

* <https://www.ncsc.gov.uk/collection/protecting-bulk-personal-data> <https://www.ncsc.gov.uk/collection/small-business-guide>
* <https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks>
* <https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing>

**4 Cyber Security**

ICT systems need to keep information confidential whilst maintaining the confidentiality, integrity, availability and resilience of the information and / or services. The degree of impact on the council from a loss of confidentiality, integrity, availability or resilience may vary and should be considered as part of a comprehensive risk assessment process. Aggregation, accumulation and association of information within ICT systems and on removable media must be considered as part of the risk management process.

Appropriate security controls should be in place for any network or systems storing council information and, in the case of information originated from the PSN these controls should be compliant with PSN Code of Connection. Personal and special category data should be stored and managed according to ISO 27001 and NCSC guidelines.

Data protection legislation has specific security obligations that need to be evidenced. These are identified as;

* Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Oldham council and any entities processing information on its behalf shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
  + the pseudonymisation and encryption of personal data
  + the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services
  + the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
  + a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing

In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

All data containing personal information whether in transit between networks/the internet, stored at rest, or in use, must be subject to the technical control measures of ISO27001 and the NCSC.

**5 Sharing Information**

Any sharing or transfer of council personal, Special or Crime data with other organisations must comply with all Legal, Regulatory and council policy requirements. In particular, this must be compliant with the Data Protection Act 2018, GDPR, The Human Rights Act 2000, Criminal Justice and Immigration Act 2008, Civil Contingencies Act 2004 and the common law of confidentiality.

Where personal and / or Special category data and / or Crime data is disclosed / shared it should only be done so on the basis of a genuine “need to know” and some information transfers / sharing may be subject to a risk / data privacy impact assessment and required documentation to provide assurance of information governance controls.

Information must only be disclosed to any other person or organisation via the most secure method available.

For instance, where information will be classed as information originating from the PSN e.g. DWP, and when sharing or transferring this ‘PSN Information’ to other organisations, this information should be assessed and categorised for handling, ensuring that any controls required by the information owner are put in place. In the absence of any controls being communicated, the person using or handling that information should attempt to classify the information according to the above guidelines.

Where information is being shared with a supplier, sub-contractor or partner for the purposes of storing or processing, the prime organisation must ensure that the 3rd party organisation recognises and understands the risks and has the systems and processes in place to comply with Oldham Council’s requirements for the handling of its information as detailed within this policy.

**6 Suppliers / Contractors Commitment**

In order to protect Oldham council information appropriately, our suppliers must provide security measures and safeguards appropriate to the nature and use of the information that they are provided with.

The supplier / partner ‘s authorised Data Controller must agree in writing to comply with these policies and standards – see Appendix 2 for a sample letter of agreement.

Each supplier must also appoint a named officer who will act as a first point of contact with Oldham council for information governance and security issues, where applicable, this must be the suppliers’ Data Protection Officer. In addition, all staff working for the supplier and where relevant sub-contractors, with access to Oldham council ICT Systems, services or Oldham council information must be made aware of these requirements and must comply with them.

Appropriate security controls should be in place for any network or systems storing Council information, minimising the risk of information loss. Personal, Special and Crime data should be stored and managed according to ISO 27001, NCSC guidelines and Data Protection Act 2018 / GDPR requirements.

All suppliers of services to Oldham council must comply, and be able to demonstrate compliance, with Oldham council’s relevant policies and standards and in the case of information originating from PSN, comply with and demonstrate compliance with any additional standards and requirements communicated to them in writing.

Whenever a processor is used (a third party who processes personal data on behalf of the controller) a written contract needs to be in place. Similarly, if a processor employs another processor it needs to have a written contract in place. The GDPR sets out what needs to be included in the contract.

Contracts between controllers and processors ensure that they both understand their obligations, responsibilities and liabilities. They help complying and demonstrating compliance with the GDPR and the Data Protection Act 2018. The use of contracts by controllers and processors may also increase data subjects’ confidence in the handling of their personal data.

Controllers are liable for their compliance with the GDPR and the Data Protection Act 2018 and must only appoint processors who can provide ‘sufficient guarantees’ that the requirements of the laws will be met and the rights of data subjects protected. In the future, this may include using a processor which adheres to an approved code of conduct or certification scheme when such schemes become available.

Processors will however have some direct responsibilities under the GDPR and may be subject to fines or other sanctions if they don’t comply.

Processors must;

* act on the written instructions of the council
* not use a sub-processor without the prior written authorisation of the council
* co-operate with the council on matters in relation to the processing
* keep records of its processing activities
* employ a Data Protection Officer if required, in accordance with Article 33 of the GDPR
* assist the council in providing subject access and allowing data subjects to exercise their rights under the GDPR
* assist the council in meeting its GDPR obligations in relation to the security of processing (article 32 of the GDPR), the notification of personal data breaches to the council as soon as it becomes aware of a breach and data protection impact assessments
* return all personal data to the controller as requested at the end of the contract; and/or delete and provide evidence of destruction/method used
* submit to audits and inspections, provide the council with whatever information it needs to ensure both are meeting their Article 28 obligations under GDPR, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state

The following are key considerations:

1. **People**
   1. Staff recruitment in accordance with regards to pre-employment checks, e.g. Baseline Personnel Security Standard (BPSS)
   2. Staff training and awareness of information security and any specific contract requirements
   3. Systems access control and a policy of least privilege
2. **Places**
   1. There should be data separation between customers, unless an information sharing agreement is in place between the customers
   2. Encrypted portable media used when transporting council information -
   3. Council information should be kept within secure premises and systems
   4. Offshoring: The council’s Personal or Marked / Categorised information must **not** be processed or stored outside the European Union without the prior written consent of Oldham council and must at all times comply with the Data Protection Act 2018
3. **Processes**
   1. Physical and electronic handling, processing and transferring of personal information, including secure access to systems, back up procedures and systems and the use of encryption
   2. The transfer of information should be carried out via secure means
   3. Ensure the secure disposal of personal information
4. **Procedures**
   1. Risk reporting procedures in place
   2. Regularly checks of policies and procedures
   3. Annual security checks / audits / tests
   4. Security incident management: includes the identification, management and agreed reporting procedures for actual or suspected security breaches

All suppliers must implement appropriate arrangements which ensure that the council’s information and any other council assets are protected in accordance with prevailing statutory and where appropriate PSN requirements. These arrangements will clearly vary according to the size of the organisation.

It is the supplier’s responsibility to monitor compliance of any sub-contractors and provide assurance to Oldham council.

Failure to comply with any of these guidelines could result in termination of the contract.

**7 Authority for this Policy**

This policy is owned by the Information Risk Assurance Manager on behalf of the council’s Senior Information Risk Officer.

This delegation is to establish and approve internal policies dealing with all aspects of the management of all Oldham Council’s information security, records and information governance.

**APPENDIX 1**

**Data Protection Principles**

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.

**APPENDIX 2**



**Personal Data Aspects Letter for Contracts involving the handling of Protected Personal Data**

**For the personal attention of:** *(Name of company Data Controller)*

Dear Sir

**TENDER NO / CONTRACT NO** *(to be inserted)*

On behalf of Oldham Council, I hereby give you notice that the Privacy Impact Assessment conducted has identified that this contract involves the requirement to handle Oldham Council Personal/Special category/Crime/PSN *(delete as appropriate)* data. This data is subject to the provisions of the Data Protection Act 2018[[1]](#footnote-2) and Security Policy Framework[[2]](#footnote-3). Your attention is also drawn to the specific aspects of data handling set out in ‘Handling Oldham Council Data’ which must be fully implemented.

Will you please confirm that:

1. This definition of the data aspects of the above contract has been brought to the attention of the person directly responsible for the protection of data in this contract.
2. The definition is fully understood.
3. Measures can and will be taken to protect the data.
4. Any problems in meeting these requirements will be notified to Oldham Council immediately.

The Provider shall indemnify and keep indemnified Oldham Council against all claims, losses, liabilities, damages, costs (including all legal fees) and expenses incurred by or awarded against the Council or for which the Council may become liable due to any failure by the Provider or its employees or agents to comply with any of its obligations under this Policy or as a result of any negligence, or breach of statute or common law by the Provider in processing the Data.

Yours faithfully

Signed on behalf of Oldham Council

……………………………………………………….

Signed on behalf of **[Please insert name of third party]** by duly authorised signatory

……………………………………………………….

|  |  |
| --- | --- |
| Name |  |
| Title |  |

Copy to: Information Manager / CIO

**APPENDIX 3**

**Caldicott Principles**

Principle 1 - Justify the purpose(s) for using confidential information

Principle 2 - Don't use personal confidential data unless it is absolutely necessary

Principle 3 - Use the minimum necessary personal confidential data

Principle 4 - Access to personal confidential data should be on a strict need-to-know basis

Principle 5 - Everyone with access to personal confidential data should be aware of their responsibilities

Principle 6 - Comply with the law

Principle 7 - The duty to share information can be as important as the duty to protect patient confidentiality

**National Data Guardian Standards**

Data Security Standard 1. All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes

Data Security Standard 2. All staff understand their responsibilities under the National Data Guardian’s Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

Data Security Standard 3. All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit.

Data Security Standard 4. Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to data subjects.

Data Security Standard 5. Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.

Data Security Standard 6. Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.

Data Security Standard 7. A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.

Data Security Standard 8. No unsupported operating systems, software or internet browsers are used within the IT estate.

Data Security Standard 9. A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.

Data Security Standard 10. IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian’s Data Security Standards.

1. http://www.legislation.gov.uk/ukpga/2018/12/contents [↑](#footnote-ref-2)
2. http://www.cabinetoffice.gov.uk/spf.aspx [↑](#footnote-ref-3)