CITY OF WOLVERHAMPTON COUNCIL

Information Governance Key Terms

Definitions, Roles and Responsibilities

Version History

Version	Date	Description	Author/Role
0.1	01/07/2021	Initial Draft.	IG Team
1.0	17/02/2022	Approval by the members of the IG Board and SEB	IG Team

Table of Contents

Definitions

The Council uses the definitions listed in the UK General Data Protection Regulation and the Data Protection Act 2018. These sources can be used to lookup official definitions, the guide below aims to give you a more user-friendly definition of some of the key Information Governance terms commonly used within the Councils Policy and Procedure documents. The Information Commissioners Office (ICO) is also a useful source of information for more guidance.

Assurance

A confident assertion, based on sufficient, relevant and reliable evidence, that something is satisfactory, with the aim of giving comfort to the recipient. The basis of the assurance will be set out and it may be qualified if full comfort cannot be given.

Breach

An act of breaking or failing to observe a law, agreement, or code of conduct or policy.

COPI (Control of Patient Information) Notice

The Secretary of State for Health and Social Care has issued NHS Digital with a Notice under Regulation 3(4) of the Health Service (Control of Patient Information) Regulations 2002 (COPI) to require NHS Digital to share confidential patient information with organisations entitled to process this under COPI for COVID-19 purposes.

Cyber Essentials/ Cyber Essentials +

Cyber Essentials is an accreditation scheme that organisations can use to demonstrate they take technical ICT security seriously and meet a set of external standards. Cyber Essentials Plus is the highest level of certification offered under the scheme. It is a rigorous test of an organisation's cyber security systems where cyber security experts carry out vulnerability tests to make sure that the organisation is protected against basic hacking and phishing attacks.

Data Breach/Personal Data Breach

Article 4 of the UK GDPR gives a definition of a personal data breach. A breach of the data protection rules means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. Breaches can be caused deliberately or accidentally.

Breaches can be due to a failure in a physical or organisational measure, for example no training on protecting data, inadequate policy and procedures on handling data, or not enough measures to stop unauthorised physical access to a filing room. They could also be caused by failures in technical measures, for example not encrypting devices where data is stored, not updating your software

causing a weakness that hackers can use to gain access to your data or allowing a virus through your organisations firewall.

Data Breaches need to be reported to the Information Governance Team and normally need to be reported on to the UK supervisory authority for Data Protection, the ICO. Please see the Councils Data Protection Policy for full details on how to manage and report these.

Data Controller/ Controller

A person, public authority, agency or other body which, alone or jointly with others, decides the purposes and means of processing personal data.

Data Processor/Processor

A person, public authority, agency or other body which processes personal data on behalf of the controller.

Data subject

An identified or identifiable living individual to whom personal data relates.

Data Protection

Data protection is about ensuring people can trust you to use their data fairly and responsibly. If anyone collects, uses or stores information about individuals for any reason other than their own personal, family or household purposes, the laws on Data Protection apply.

Data Protection Laws

The UK data protection laws are set out in the Data Protection Act 2018 (DPA), along with the UK General Data Protection Regulation (GDPR). It takes a flexible, risk-based approach which puts the onus on Controllers to think about and justify how and why they use data.

Data Protection Act 2018

The UK law on how data should be handled securely fit for the digital age when an ever increasing amount of data is being processed, and it empowers people to take control of their own data. Data Protection Act 2018 (legislation.gov.uk)

Data Protection Principles

a) **Lawfulness, fairness and transparency** - Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency.
b) **Purpose limitation** - collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

c) **Data minimisation** - adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation).
d) **Accuracy** - 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').
e) **Storage limitation -** kept in a form which permits identification of data subjects for no longer than is necessary.
f) **Integrity and confidentiality (security)** - 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.
g) **Accountability -** First, the accountability principle makes it clear that you are responsible for complying with the UK GDPR. Second, you must be able to demonstrate your compliance.

Data Portability

The ability to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without affecting its usability. Data Portability is one of the data rights individuals have under the Data Protection Act 2018, and UK GDPR.

DPA/Data Processing Agreement

A data processing agreement is a legally binding contract that states the rights and obligations of each party concerning the protection of personal data. They are put in place between one or more organisations where they have a relationship due to the processing of the data.

DPIA/ Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) is a process to help you identify and minimise the data protection risks of a project

Data Rights

Under the Data Protection legislation, data subjects have the following rights with regards to their personal information:

- the right to be informed about the collection and the use of their personal data.
- the right to access personal data and supplementary information.
- the right to have inaccurate personal data rectified or completed if it is incomplete.
- the right to erasure (to be forgotten) in certain circumstances.
- the right to restrict processing in certain circumstances.
- the right to data portability, which allows the data subject to obtain and reuse their personal data for their own purposes across different services.

- the right to object to processing in certain circumstances.
- rights in relation to automated decision making and profiling.
- the right to withdraw consent at any time (where relevant).
- the right to complain to the Information Commissioner.

DSA/ Data Sharing Agreement

Data sharing agreements set out the purpose of the data sharing, cover what happens to the data at each stage, set standards and help all the parties involved in sharing to be clear about their roles and responsibilities.

DSPT (Formerly the IGToolkit)

The Data Security and Protection Toolkit is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards. All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.

EIR

The Environmental Information Regulations 2004 The Environmental Information Regulations 2004 (legislation.gov.uk)

Erasure

The UK GDPR introduces a right for individuals to have personal data erased. The right to erasure is also known as 'the right to be forgotten'. The right is not absolute and only applies in certain circumstances.

Exemption

An exemption is a legally defined reason that means the Council may not need to respond to requests made under the Freedom of Information Act 2000 (FoIA) or Data Protection Act 2018/UK GDPR.

Exception

An exception is a legally defined reason that means the Council may not need to respond to requests made under the Environmental Information Regulations (EIR).

FoIA/ FOI

Freedom of Information Act 2000 Freedom of Information Act 2000 (legislation.gov.uk)

GDPR/ UK GDPR/ General Data Protection Regulation

GDPR - is a European regulation that requires significant protections for how organisations gather, use and manage personal data if it affects EU citizens. General Data Protection Regulation (GDPR) – Official Legal Text (gdpr-info.eu)

UK GDPR - sits alongside an amended version of the DPA 2018. The key principles, rights and obligations remain the same. However, there are implications for the rules on transfers of personal data between the UK and the EEA. The UK GDPR also applies to controllers and processors based outside the UK if their processing activities relate to UK citizens. https://www.legislation.gov.uk/eur/2016/679/contents

Governance

The arrangements in place to ensure that the Council fulfils its overall purpose, achieves its intended outcomes for citizens and service users and operates in an economical, effective, efficient and ethical manner.

ICO/ Information Commissioner Office

The Information Commissioner Office, the supervisory authority responsible for overseeing Data Protection and Freedom of Information in the UK.

IGB/ Information Governance Board

The governance group charged with carrying out assurance work and implementing and monitoring IG controls across the organisation.

Information Asset/ Information Asset Register (IAR)

An Information Asset Register (IAR) is a catalogue of the information we hold and process, where it is stored, how it moves and who we share it with. We need to know what the data is to understand how we need to protect it and decide long we can and should keep data for.

Information Asset Owners (IAO)

Has overall responsibility for the datasets and information assets used within their service area/department. This role is usually taken on by a Manager or Head of Service. They are responsible for having oversight of and maintaining an up to date Information Asset Register for their service area/department. This includes assessing information risk for their datasets and being the escalation point for the Information Asset Administrator to raise any issues.

Information Asset Administrator (IAA)

Will be responsible for the day-to-day management of data set or asset. They will be responsible for approving who can have access to the asset and implementing appropriate controls and data quality measures. They are best placed to recognising and reporting actual or potential security incidents related to the information assets.

Information Incident

This is a lower level data breach that needs to be reported internally to the Council's Information Governance Team, to review and identify if there are any trends in the types of incidents being report and take remedial action across the Council to address them. The consequences of an incident are normally not further reportable to the UK supervisory authority on Data Protection, the ICO. Please see the Council's IS05 Information Incident Management Policy for full details on how to manage and report these.

Internal Review

Under the FOI and EIR regimes, if a person is unhappy with the Councils initial response they can ask for an internal review. This is where an officer not involved in the case will look at the response and any exemptions applied to comment on whether the response was sufficient or recommend and carry out any further actions to address the issues raised. The response time for an internal review is 20 working days under both EIR and FOI and can be extended up to a maximum of 40 working days.

Legal Basis for Processing

A lawful basis is the reason or legal grounds you can rely on for using People's personal data. There are six bases to choose from:

- consent;
- contract;
- legal obligation;
- vital interests;
- public task; and
- legitimate interests.

There's no single lawful basis that's better or more lawful than any of the others. It's up to the data controller to choose which is most appropriate for what they're doing with data.

National Data Opt-Out (Section 251)

The national data opt-out gives everyone the ability to stop health and social care organisations from sharing their confidential information for research and planning purposes, with some exceptions such as where there is a legal mandate/direction or an overriding public interest for example to help manage the covid-19 pandemic. More detail can be found here: Section 251 and the application of national data opt-outs - NHS Digital

Object to processing

This is one of the data rights individuals have. The right to object means people can object to specific processing of their personal data, so you'd have to stop using their data for certain purposes unless you have a legal reason to continue. For example, if a customer objects to you using their details to send them postal marketing, you

could suppress or flag their details, so you know not to post them marketing material again.

Personal data

Any information relating to a person (a 'data subject') 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 person.

PIT/ Public Interest Test

This is a test that must be done when you consider applying some exemptions under the Freedom of Information Act 2000. Some exemptions under the Freedom of Information Act are 'absolute' and some are 'qualified'. If the exemption is qualified, the public authority must weigh the public interest in maintaining the exemption against the public interest in disclosure. This is the public interest test.

Principles/ Data Protection Principles

The UK GDPR sets out seven key principles of data protection, the Data Protection Act 2018 also refers back to these. They should lie at the heart of organisations approach to processing personal data.

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
- Accountability

Privacy Notice

A privacy notice is sometimes known as 'fair processing information', 'privacy information', or a 'privacy policy'. All of these terms refer to information about why you hold people's personal data. Data Protection Laws (DPA and UK GDPR) require that organisations who process personal data must provide the public with a privacy notice. It also states that it must include a standard set of information such as the DPO contact details, how people make a data rights request, what you plan to do with the data you hold, how long you're going to keep it, and if you'll share it with anyone else. Privacy and Cookies Notice | City Of Wolverhampton Council

Processing

In relation to personal data, means any operation or set of operations which is performed on personal data or on sets of personal data (whether or not by automated means, such as collection, recording, organisation, structuring, storage,

alteration, retrieval, consultation, use, disclosure, dissemination, restriction, erasure or destruction).

PSN/ PSN Certificate

The Public Services Network (PSN) is the UK government's high-performance network, which helps public sector organisations work together, reduce duplication and share resources. It unified the provision of network infrastructure across the United Kingdom public sector into an interconnected "network of networks" to increase efficiency and reduce overall public expenditure.

A PSN Certificate is needed before an organisation can connect to the PSN network, to ensure all organisation who connect deliver the same high level of security, and do not place any other organisation at risk of cyber-attack.

Rectification

Under Article 16 of the UK GDPR individuals have the right to have inaccurate personal data rectified. An individual may also be able to have incomplete personal data completed – although this will depend on the purposes for the processing. This may involve providing a supplementary statement to the incomplete data

Restrict Processing

Article 18 of the UK GDPR gives individuals the right to restrict the processing of their personal data in certain circumstances. This means that an individual can limit the way that an organisation uses their data. This is an alternative to requesting the erasure of their data.

Risk/Information Risk

An informaiton risk is the possibility or potential for vital or key informaiton that the Council holds being misused, disrupted, lost, stolen, corrupted, modified or destroyed without authorisation. Such incidents can threaten peoples privacy, disrupt business, damage assets and facilitate other crimes such as fraud and may result in a risk of financial penalty for the Council.

Risk Management

A logical and systematic method of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating the risks associated with any activity, function or process in a way that will enable the organisation to minimise losses and maximise opportunities.

ROPA/ Record of Processing Activities

AROPA is a record of an organisation’s processing activities involving personal data. Pursuant to Art. 30 (3) GDPR, it must be in written or electronic text form.

“Processing” is any activity performed on personal data and is not only the active collection of data but also the mere storage of data on a server is considered processing. In practise, each business process will be a separate processing activity.

SAR/ Subject Access Request

Under the Data Protection Act 2018 (DPA 2018) individuals have the right to access and receive a copy of their personal data, and other supplementary information. This is commonly referred to as a subject access request (SAR).

SEB

The Councils Senior Executive Board.

Roles and Responsibilities

Senior Executive Board

The Strategic Executive Board and Managing Director have overall responsibility for ensuring appropriate resources are in place.

Information Governance Board

Responsible for overseeing the Councils policy and strategy in respect of data protection taking into account any legal and local authority requirements, and ensuring it is effective in terms of resource, commitment and execution and is being appropriately communicated to staff.

Chief Executive (CE)

Overall accountability and responsibility for all aspects of governance across the Council. They provide leadership and direction to the staff of the Council in terms of Information Governance as a whole. They are required to provide assurance that all data risks to the Council are effectively managed and mitigated. They will delegate responsibility for Information Risk to the SIRO and compliance with the Data Protection Responsibilities to the DPO.

Senior Information Risk Owner (SIRO)

Is a member of the Senior Executive Board with overall responsibility for an organisation's information risk policy. The SIRO is accountable and responsible for information risk across the organisation. The SIRO will lead and foster a culture that values, protects and uses information for the benefit of both the authority and its customers. They have overall responsibility in ensuring that information threats and data security breaches are identified, assessed and any data breaches managed. They will ensure that the Chief Executive, Data Protection Officer and the Information Governance Board are fully briefed on all information risk issues to the authority.

The Senior Information Risk Owner (SIRO) chairs the Information Governance Board and has overall responsibility for managing information risk. Information Governance issues are reported to the Board by the Information Governance Team and progress on records management is reported on a regular basis by the Records Manager.

Monitoring Officer

The Monitoring Officer has the specific duty to ensure that the Council, its officers, and its Elected Councillors, maintain the highest standards of conduct in all they do. The main duties of the Monitoring Officer are set out below. The Monitoring Officer's legal basis is found in Section 5 of the Local Government and Housing Act 1989 (as amended).

Caldicott Guardian

The Caldicott Guardian(s) for Social Care are responsible for ensuring that the Council upholds the highest practical standard for handling personal and sensitive data, the safeguarding of information processed for social care work and will oversee all procedures for protecting the confidentiality of service user information and enabling the appropriate information sharing.

The Caldicott Guardians will ensure that compliance with this policy is achieved and will work proactively (supported by nominated staff) to ensure that personal data processed for social care is appropriately safeguarded to meet the requirements of the DPA 2018, and other relevant legislation.

The Caldicott Guardians will provide advice, guidance and expertise to the Information Governance Board in relation to social care service user information and will support the Information Governance structures in place within the Council.

Social Care Caldicott Guardians are responsible for ensuring that personal identifiable information is protected and shared appropriately.

Data Protection Officer (DPO)

Data Protection Officer is a statutory role as mandated by the UK General Data Protection Regulations and the Data Protection Act 2018. All organisations who process personal/sensitive data must have this role in place to oversee an organisation’s data protection strategy and implementation. They are the officer that ensures that an organization is complying with data protection requirements.

The DPO’s role is to inform and advise the data controller or the processor and the employees who carry out processing of their obligations in line with relevant data protection law;

The DPO will:

- Monitor compliance with the Data Protection Act 2018 and the UK General Data Protection Regulations (UK GDPR) and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
- Provide advice where requested as regards the data protection impact assessment (DPIA) and monitor its performance pursuant to Article 35;
- Cooperate with the Supervisory Authority; this being the Information Commissioner's Office (ICO);
- Act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter;
- Shall perform their duties in an independent manner with due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Directors/Managers

Directors and managers are responsible for ensuring they manage the records relating to their business areas in accordance with records management policy and procedures. They must ensure any new employees or contractors are made aware of the policy and undertake relevant information and records management training. They must ensure any potential risks to compliance are identified, assessed, recorded and appropriately mitigated and managed

Information Governance Manager

The information Governance Manager will ensure there are resources and mechanisms are in place to manage requests for access to information under Data Protection legislation, and the wider Information Governance Framework.

The role is also responsible for ensuring that the Council is registered with the Information Commissioner's Office for data processing, that the registration accurately reflects the data processing activities undertaken by the Council and that the registration is maintained and renewed as required.

The role will ensure appropriate Data Protection training is developed and delivered to Council employees.

Information Governance Team

Are made up of a strategic section who deal with ongoing compliance and monitoring, advice and guidance and supporting Leadership Teams across the Council in maintaining compliance with the various information legislative requirements placed upon the council. There is also a transaction team who deal with day to day requests for information under the relevant information governance laws.

Qualified Person

The qualified person is defined by section 36 (5) of the Freedom of Information act 2000, in relation to the approval of section 36 exemptions under the same act.

Resilience Manager

The Resilience Manager is responsible for coordinating business continuity planning and working with service managers and the Records Manager to identify and safeguard priority business areas, systems and vital records.

Digital and IT

The Digital and IT departments is responsible for data storage, backup and disaster recovery for in-house systems which hold the Council's electronic records. They are responsible for keeping systems, up to date, backed up and patched with the most recent software to ensure the greatest protection from hacking and phishing and other cyber threats.

RIPA Senior Responsible Officer

Is responsible for overseeing the Council abides by the legislative requirements of the Regulation of Investigatory Powers Act 2000 (RIPA). Ensuring that the RIPA techniques that are used in a regulated way and provides safeguards against the abuse of such methods. Authorise and approve the use of covert techniques so that they are considered legal, necessary and proportionate.

CCTV Control Manager

Responsible for overseeing the management and use for surveillance of Council controlled CCTV systems. Escalating issues to Senior Management and the RIPA Senior Responsible Officer/SIRO where applicable.

Archives Staff

Staff at the City Archives have responsibility for preserving some records which need to be kept in the long term including historical records deemed worthy of permanent preservation.

Information Asset Owners/ IAO

Information Asset Owners (IAOs) must be senior/responsible individuals involved in running the business/service area. Each directorate will designate an Information Asset Owner (IAO) to take responsibility for the correct protection and handling arrangements for the information assets 'owned' by them.

Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. IAOs are also responsible for ensuring that services implement all information governance policies and their supporting processes as set out in the Information Governance Policy.

Where the processing of personal information is quite complex - for example - in relation to health and social care, directorates should draw up specific data protection guidance for their directorate which is aligned with, and supports, this policy. This may include specific operational procedures, including directorate induction and training, to ensure that detailed data protection practice is established and followed.

As a result, they are able to understand and address risks to the information and ensure that information is fully used within the law for the public good. They provide a written judgement of the security and use of their asset annually to support the audit process.

Information Asset Administrators/IAA (system administrators)

An Information asset administrator (IAA) may be responsible for the day-to-day management of data within a service. The Information Asset Owner (IAO) may delegate responsibility for management of confidential information in particular databases, systems or workstreams to one or more Information Asset Administrators (IAA). Delegated responsibilities typically include:

- Managing the joiners, movers and leavers process within the team
- Ensuring all team members keep their training up-to-date
- Granting and revoking access to confidential information
- Recognising potential or actual security incidents
- Consulting the IAO on incident management
- Ensuring that risk assessments and other documents for the data are accurate and maintained

The Information Asset Owner (IAO) remains ultimately responsible.

Managers

All managers are:

- Required to ensure that they (and their staff) understand and adhere to this policy and any associated procedures.
- Responsible for ensuring that staff are informed and updated on any changes made to this policy.
- Identify and report any risks or breaches to the security of personal data processed by the Council to their relevant line manager or appropriate Information Asset Owner.
- Must ensure that their staff undertake information governance training and any training in data protection/information security which is specific to their role. Refresher training will be undertaken annually.

Staff

Everyone who is employed by the Council (permanent and temporary members of staff, agents, contractors and consultants) has a responsibility work within accordance with the Council’s policies, standards, procedures and guidelines.

- Have a responsibility for data protection and are required to adhere to this policy, any associated procedures;
- To attend any associated data handling, protecting information, or Data Protection training;
- All staff must understand the main concepts within the legislation, and raise any queries to their line manager or the Information Governance Team for advice and guidance;
- Identify and report any risks to the security of personal data processed by the Council to their line manager or the Information Asset Owner or the Councils DPO;
- Assist their customers/service users to understand their rights and the Council's responsibilities in regards to data protection;
- Identify and report any subject access requests to the IG Team or so that they can be processed in accordance with the law.