Information Governance Policy

Keeping information about customers and employees safe and secure and using it to help improve the services we provide.

Version: V1.0 Final
Version Date: November 2020
Revision Date: November 2022

Contents

Policy Statement

This Policy establishes the key high-level principles of information governance and data protection in Walsall Council. It provides an overarching direction that ensures all staff are aware of their duties and obligations as set out by the Data protection Regulations and Legislation by ensuring, all staff are fully supported through a framework of Information Governance Standards, Procedures and Guidance that are embedded into our working practices and data processing activities.

This Policy and the Information Governance Standards, Procedures and supporting Guidance apply to all employees, elected members and anyone else working for or on behalf of the council i.e. partners, contractors and agents.

To this end, the council commits to:

Information Governance Management: supporting robust operational and management accountability structures, with appropriate resources and expertise to ensure information governance and data protection compliance issues are dealt with appropriately, effectively and at levels within the organisation commensurate with the type and gravity of the issue in question.

Staff Empowerment: embedding a culture of individual responsibility and capability across the council in relation to information management, protection and use as part of 'business as usual'.

Training and Awareness: maintaining a system of training and awareness that meets government and contractual mandatory requirements, and is capable of equipping employees with the skills and knowledge necessary to do their jobs and respond to customer demand while complying with the General Data Protection Regulations 2016, UK Data Protection Act 2018 alongside Information and Cyber Security Standards or requirements.

Systems and Processes: establishing and maintaining information systems and processes to enable the efficient and secure storage and retrieval of information and the management of information risk.

Policy and guidance: developing and embedding, standards, procedures and guidance documents in relation to the respective areas of information governance that support employees to fully understand the duties and responsibilities required to ensure the council continues to comply with its legal obligations.

1. Applying the Policy

In approving this Information Governance Policy, the council recognises and supports:

- the principle that accurate, timely and relevant information is a legal requirement and essential to deliver high quality services and that it is the responsibility of anyone working for or on behalf of the council to ensure and promote the quality of information and to actively use information in decision-making processes
- the need for an appropriate balance between openness and confidentiality in the management and use of information
- that the principles of corporate governance and public accountability place equal importance on the confidentiality of, and the security arrangements to safeguard, both personal information about customers and employees and commercially sensitive information
- the need to share information with other organisations in a controlled and secure manner consistent with the interests of the customer and, in some circumstances, the public interest.

2. Senior Roles and Responsibilities

The Information Governance Structure is led by a corporate group – the Forum for Information Governance & Assurance (FIGA), which is accountable to the Corporate Management Team.

Membership of the Forum consists of Information Champions who hold senior roles in the council and seek to champion the principles and requirements of information governance across the council.

The Forum is chaired by the SIRO and or Data Protection Manager and requires attendance by directorate level information champions, legal and HR representatives, the Information Security Officer, directorate representatives and the information governance and assurance officers alongside any other representation as required or appropriate for ensuring compliance of the regulations is upheld.

FIGA is responsible for ensuring that Information Governance Policies, Standards, Procedures or Guidance are reviewed and maintained as well as ensuring that any Information risks identified are addressed and actioned accordingly.

The group also provides assurance to the Chief Executive, Corporate Management Team and elected members that the organisation takes information management and governance seriously and can demonstrate visible improvements through a risk-based approach and regular reporting requirements, which ensure appropriate levels of accountability are in place throughout the council.

Roles	Responsibilities
Senior Information Risk Owner (SIRO)	Is accountable for information risks, fostering a culture for protecting and using data appropriately and provides senior responsibility for managing information risks and incidents and is concerned with the management of all information assets.
Caldicott Guardian	Is advisory and acts as the conscience of the organisation. Provides a focal point for customer confidentiality & information sharing issues. Is concerned with the management and sharing of personal information.
Data Protection Manager	The Data Protection Manager ensures that the council has adopted good information governance policies and procedures and complies with data protection laws. This function will also act in an advisory capacity to the Chief Executive, Caldicott Guardian and SIRO were required. This function will be delivered through the role of the 'Data Protection Manager', which also acts the Data Protection Officer for the council in its statutory function.
Information Security Officer	Responsible for developing, implementing and reviewing policies and procedures to protect the councils network and information assets, providing advice and guidance on information and cyber security. The role will also input into general user awareness and training and is responsible for data and cyber security initiatives generally.
Information Governance and Assurance Officer(s)	Responsible for developing, implementing and enforcing policies and procedures to ensure correct information and records management practice across the council. Delivering reports to FIGA that cover the requirements for data processing, information assets, and assessment/audit outcomes alongside regulatory compliance. The role is also responsible for ensuring compliance with information governance awareness training and the delivery of appropriate training throughout the authority.
Information Champions	This role is responsible for ensuring data protection breaches are managed and directorates are accountable for any required actions or risks identified though the incident management process. They act as the key link between the information governance team and the directorate senior leaders to ensure that the councils remains compliant with its legal duties and responsibilities for accountability. They Champion data protection awareness, understanding and compliance with the key principles of information governance within the directorate. As members of FIGA they are responsible for ensuring key messages and actions are disseminated appropriately throughout the directorates.
Information Asset Owners	Accountable senior officers with ownership and responsibility for information assets (paper based and electronic records and IT systems) within their directorate. IAO's must identify and document within the information asset register, the availability and compliance requirements for their systems and formulate a contingency plan in the event of system failure. Supported by Information Asset Custodians and champions.

Information Asset Custodians	Designated officer with responsibility for day-to-day management, administration and protection of specified information assets (paper-based records and IT systems).

3. Strategic Implementation

FIGA will monitor implementation of this Policy and associated documents through regular meetings, which will involve:

- ensuring any Standards and procedures or guidance required for compliance of obligations are developed, reviewed and monitored while being responsible for the approval of these documents through the directorate leads and champions.
- ensuring appropriate resources are in place to achieve compliance of the regulatory requirements
- reporting on progress, incidents and issues to accountable senior level positions including CMT/elected members.

This Policy will be reviewed biennially and approved by FIGA, CMT and the council's full Cabinet.

4. Governance and Compliance

Non-compliance with this Policy and the associated Information Governance standards, procedures or guidance could potentially expose the council and/or its customers to significant levels of risk. The potential impact of such risks through the damage, unauthorised disclosure or loss of information includes but is not limited to:

- disruption to services,
- the risk of harm or distress to citizens,
- damage to the organisational reputation,
- legal action,
- monetary penalties,
- personal distress,
- loss of confidence,
- or media coverage

and may take considerable time and cost to recover from.

5. Responsibilities

The Data Protection Manager shall have overall responsibility for managing and implementing the Information Governance Policy and accompanying Standards and procedures on a day-to-day basis.

Line Managers are responsible for ensuring that their permanent and temporary employees and contractors have:-

- read and understood the Information Governance Policy and the Standards and procedures applicable in their work areas
- been made aware of their personal responsibilities and duties in relation to information governance
- been made aware of who to contact for further advice and where to locate any guidance
- received appropriate and up-to-date training relating to information governance
- abide by the council's Code of Conduct

Line Managers are also responsible for ensuring that any information or data processing undertaken by their service area or team complies with both the data protection and records management requirements or standards and that staff have been made aware of the top level principles of good information governance in that records must be:

- Adequate, relevant and not excessive
- contain the minimum information required for the specified purpose
- that appropriate privacy notices ensure transparency over any data processing activity
- justified, lawful and available on a need to know basis only

All staff are responsible for ensuring that they comply with the data protection principles and standards in that they are directly responsible for respecting and upholding confidentiality, using information for the purpose for which it was collected and sharing or accessing information in a secure and adequate manner on a need to know basis only.

All Staff must comply with the Standards, Procedures and Guidance that forms part of this policy

Non-compliance with this policy and the Information Governance Standards, Procedures or guidance may therefore be subject to performance or disciplinary action, in line with the council's disciplinary procedures and or legal action where appropriate.

The following table identifies who within Walsall Council is Accountable, Responsible, Informed or Consulted concerning this Policy. The following definitions apply:

- **Accountable** – the person who has ultimate accountability and authority for the Policy.
- **Responsible** – the person(s) responsible for developing and implementing and reviewing the Policy and any associated Standards, procedures or Guidance.
- **Consulted** – the person(s) or groups to be consulted when the Policy is reviewed and approved
- **Informed** – the person(s) or groups to be informed throughout the approval process.

Accountable	Senior Information Risk Owner
Responsible	Data Protection Manager
Consulted	Forum for Information Governance & Assurance (FIGA)
Informed	All individuals employed by the council either permanently, on a temporary basis or as a contractor, elected members and partner organisations

Document History

Revision Date	Version	Revised By	Summary of Changes
19/10/2020	0.1 Draft	C. Hobbs	Policy extracted from Information Governance Framework Standards 2018.
30.11.2020	1.0 Final	P.Withers	Policy amended and edited to ensure responsibilities and duties align to the legal requirements.

Approvals

This Policy has received the following approvals:

Name	Title	Signature	Date of Approval
Forum for Information Governance & Assurance (FIGA)		As minuted	27.10.2020
Corporate Management Team (CMT)		As minuted	23.22.2020
Cabinet		APPROVED	09.12.2020

Appendix 1 – Legal Requirements, Regulations and Standards

The council and all individuals working for or on behalf of the council are governed by a number of laws, regulations and standards relating to information governance. These include but are not limited to:

- Access to Medical Records Act 1990
- Caldicott Review 2017
- CCTV Code of practice 2017
- CCTV Code of conduct 2019
- Children and Families Act 2014
- Civil Evidence Act 1995
- Code of practice for legal admissibility and evidential weight of information stored electronically BIP0008:2014
- Common law duty of confidence
- Computer Misuse Act 1990
- Copyright, Designs and Patents Act 1988
- Data Protection Act 2018
- Environmental Information Regulations 2004
- Freedom of Information Act 2000
- General Data Protection Regulations (GDPR) 2016
- Health and Safety at Work Act 1974
- Health and Social Care Act 2001
- HMG Security Policy Framework 2014 (v1.1 May 2018 to take account of GDPR)
- Human Rights Act 1998
- International Standard for Information and Documentation, Records Management
- International Standards for Information Security - ISO27001:2013 & ISO27002:2013
- Investigatory Powers Act 2016
- ISO 15489
  Records Management Code of Practice for Health and Social Care 2016
- ISO 27001 Information Security Management Standards
- ISO 27032:2012 Information technology Security techniques - Guidelines for cyber security
- Local Government Act 1972 (Section 224)
- Mental Capacity Act 2015
- NHS Confidentiality Code of Practice 2016
- PCI/DSS
- Safeguarding Vulnerable Groups Act 2006UK Data Protection Act 2018

Appendix 2 - Related Council Standards, Procedures and Guidance

- Account Access Request Procedure
- Agile Working Policy
- Data Breach Handling Procedure
- Data Change Request Procedure
- Email Retention Guidance – A Quick Guide to Managing Emails
- Information Rick and Security Standard
- Information Rights Standard
- Records Management Standard