

## **Cabinet – 13 March 2013**

### **Information Governance Policy Framework**

**Portfolio:** Councillor Arif, Business support services

**Related portfolios:** Councillor Towe, Cllr Adrian Andrew

**Service:** Programme Delivery & Governance

**Wards:** All wards

**Key decision: No**

**Forward plan: No**

#### **1. Summary**

The report provides information relating to the new Information Governance strategy - a Framework of 3 Policies, Information Risk & Security Policy, Information Rights Policy and Records Management Policy), which are for consideration by Cabinet.

The Information Governance strategy sets out the legal requirements which the Council is obliged to follow with regard to Information Governance (IG) and confirms the Council's commitments to these requirements. It also recognises customers at the heart of Council business and brings together recognition of new ways of working and developing services to better meet customer need. This Policy also establishes a culture of individual responsibility for Information Governance, informed and supported by awareness and training for staff, Councillors and others working on behalf of the Council. This will enable all to understand the importance of information governance, know their responsibilities, and manage information appropriately.

As part of this strategy the Council has also established a Forum for Information Governance & Assurance (FIGA), a board that meets quarterly with the purpose of providing assurance to the Chief Executive and Corporate Management Team on how the council is dealing with information management and addressing issues following a risk-based approach. FIGA is attended by senior managers from each Directorate and representatives from Risk, Audit and Legal Services and is supported by an internal structure comprising of the Senior Information Risk Owner (SIRO), Caldicott Guardian, Information Asset Owners, Information Asset Custodians and the Information Governance & Assurance Team. This structure along with the policy framework will help to ensure that staff are able to deliver the requirements relating to information Governance.

## 2. Recommendations

- 2.1 That Cabinet approve the Information Governance Policy Framework in its entirety including all three Policies.
- 2.2 That Cabinet acknowledge that steps are being taken within the Council to improve awareness and ensure that all staff and Members receive appropriate training to support the implementation and delivery of this Policy Framework.
- 2.3 That Cabinet acknowledge that:

Employees who do not comply with these policies may be subject to Disciplinary action, in line with the Councils Disciplinary Procedures.

Members' failure to complete the required Protecting Information training and with comply with these Policies could result in the Council being unable to lawfully share Personal information with Members. A failure to comply with the Policies may also constitute a breach of the Member's Code of Conduct.

## 3. Report detail

### 3.1 Background

Cabinet previously approved the Council's Data Protection Protocol and the Information Security Procedures in 2008. However, since this time the Council has experienced a number of significant breaches of the data protection act and has been required to sign an Undertaking from the Information Commissioners confirming the Council's commitment to complying with the requirements of the Data Protection Act.

Following the issue of the Undertaking, the Corporate Management Team approved the establishment of the Information Management to review current processes and procedures and to ensure that areas of high risk were identified and addressed across the Council. The project has been running for 14 months and has identified a number of weaknesses with regard to clear, robust and seamless Policies, an absence of staff awareness and training, measures to support safe and secure, storage use and sharing of Information Assets.

The Project has also worked to develop guidance and support activities which enable increased opportunities for working in partnership with others, through the safe and secure sharing of information to support improved service delivery and better outcomes for customers.

### 3.2 Information Governance Policy Framework

The Information Governance Policy Framework (IGPF) is addressed in three parts:

**Part 1: Information Risk & Security Policy** – including confidentiality, information sharing and privacy impact assessments.

**Part 2: Information Rights Policy** - including Freedom of Information, Environmental Information Regulations, and the Rights of Data Subjects under the Data Protection Act 1998 (subject access, objection to processing and amendments to inaccurate records).

**Part 3: Records Management Policy** – including Information Quality Assurance.

These Policies will ensure that there is a robust framework relating to the obtaining, recording, holding, using, sharing and destruction of all data and records held or used by the Council and ensuring that relevant and accurate information is available where and when it is needed to improve service delivery to customers. It will also ensure that measures are in place to reduce the occurrence of breaches in information security.

#### **4. Council priorities**

Adopting this approach will support the vision and priorities of the Corporate Plan and Working Smarter initiative through overall improvements to the identification, storage, protection and efficient use of Information Assets and facilitate the transition of Public Health into the Council from April 2013.

##### **4.1 Related Portfolio Holders:**

The Information Governance Policy Framework applies to all Council employees. Employees who do not comply with these policies may be subject to Disciplinary action, in line with the Council's Disciplinary Procedures. The policies are also concerned with the new improved working practices and associated physical risks and security measures required to ensure that information assets are stored and accessed appropriately from and within all Council locations.

#### **5. Risk management**

The Information Governance Policy Framework has been developed using a risk based approach. By prioritising effort and resources on services within the council where there is the greatest potential for significant detriment to customers and the Council. The implementation of this framework will ensure consistency across the Council.

The Information Management project has appointed an Information Risk and Security Officer to identify and assess current ways of working to mitigate risks. The SIRO and the Information Asset Owners are required to ensure that there are plans in place to identify, record and manage risks to information assets, including breaches of the Data Protection Act that could result in financial penalties, damage to Council reputation and or potential detriment to customers. These will be reported to and monitored by FIGA.

The use of Privacy Impact Assessments will also ensure that where changes to processes or business activity may have an impact on privacy, risks are identified and addressed promptly.

## **6. Financial implications**

There are no financial implications arising directly from this report.

## **7. Legal implications**

Information Governance is underpinned by a number of legislative requirements which are set out in **Appendix 1** of the Information Governance Policy Framework. Failure to adhere to these requirements could result in potential financial penalties, criminal prosecution and / or an inability to deliver key services.

## **8. Staffing implications**

Information Governance is relevant to all members of staff and elected Members specific training and awareness raising will ensure that all staff are aware of their responsibilities in these respects. The Information Governance & Assurance Team will act as a central source of advice and guidance to all staff including the SIRO and Caldicott Guardian.

## **9. Equality implications**

None

## **10. Customer Impact**

Where it is considered that changes to processes or business activity could have an impact on privacy, the use of Privacy Impact Assessments will involve consultation with stakeholders and customers. To ensure that risks to privacy are identified and addressed promptly and that proposed changes to services deliver positive benefits to customers.

## **11. Consultation**

The Forum for Information Governance & Assurance have reviewed and approved these policies. Membership of FIGA includes representatives from Legal Services, Risk & Insurance the Caldicott Guardian and the Senior Information Risk Owner.

The Policy Framework has also been shared with the unions via the Employee Relations Forum and the Corporate Management Team

## **Background papers**

None

## Author

Nailah Ukaidi

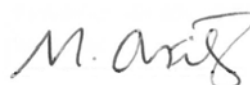
☎ 650970

✉ ukaidin@walsall.gov.uk

Handwritten signature of Rory Borealis, consisting of the letters 'R' and 'B' with a stylized flourish.

Rory Borealis  
Executive Director

5 March 2013

Handwritten signature of Councillor Arif, written in a cursive style.

Councillor Arif  
Portfolio holder

5 March 2013



# Information Governance Policy Framework

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

---

Authors: Nailah Ukaidi  
James Sparrock  
Colin Teasdale  
Version: V 0.3  
Status: DRAFT  
Version Date: February 2013  
Revision Date: March 2014



**Contents**

1.0 Policy Statement..... 5

2.0 Purpose..... 6

3.0 What is Information Governance? ..... 7

4.0 Applying the Policy Framework..... 7

5.0 Delivery..... 7

6.0 Information Governance roles and responsibilities ..... 10

7.0 Strategy implementation..... 11

8.0 Governance and compliance ..... 11

    8.1 Employees..... 11

    8.2 Elected Members/Councillors ..... 11

    8.3 Others working on behalf of the council ..... 12

    8.3 Responsibilities ..... 12

Part 1: Information Risk and Security Policy ..... 13

    1.1 Policy Statement..... 13

    1.2 Scope ..... 14

    1.3 The Policy..... 14

        1.3.1 Information Assets & Risk Management ..... 14

        1.3.2 Information Asset Security & Confidentiality ..... 14

        1.3.3 Information Sharing ..... 15

        1.3.4 Systems Development, Planning and Procurement ..... 15

        1.3.5 Contracts..... 15

        1.3.6 Contracts of Employment..... 15

        1.3.7 Business Continuity Planning..... 15

        1.3.8 Intellectual Property Rights ..... 15

        1.3.9 Personal Use ..... 16

        1.3.10 Breach Management ..... 16

Part 2: Information Rights Policy ..... 17



2.1 Policy Statement.....	17
2.2 Scope .....	17
2.3 The Policy.....	17
2.3.1 Freedom of Information (FOI)/Environmental Information Regulations (EIR).....	17
2.3.1.1 Making a request .....	17
2.3.1.2 Environmental Information Regulations .....	18
2.3.1.3 Advice and assistance .....	19
2.3.1.4 Handling Requests .....	19
2.3.1.5 Timing of Requests .....	19
2.3.1.6 Refusing a request .....	19
2.3.1.7 Qualified Person .....	20
2.3.1.8 Consultation with third parties.....	20
2.3.1.9 Contracts.....	20
2.3.1.10 Repeat requests.....	20
2.3.1.11 Publication scheme.....	21
2.3.2 Subject Access Requests.....	21
2.3.2.1 Confirming Identity.....	21
2.3.2.2 Handling Requests .....	21
2.3.2.3 Timing of Requests .....	21
2.3.2.4 Access to Personal Data by an authorised / legal agent .....	22
2.3.2.5 Access to Personal Data of a Child.....	22
2.3.2.6 The Mental Capacity Act.....	22
2.3.2.7 Information containing third party data.....	22
2.3.2.8 Access to records of deceased individuals .....	22
2.3.2.9 Refusing a request .....	22
2.3.3 Privacy Notices.....	23
2.3.4 Amendments to inaccurate records .....	23
2.3.5 Objections to Processing.....	23
2.3.5.1 Direct Marketing.....	23
2.3.5.2 Prevention of processing likely to cause substantial damage or distress .....	23
2.3.6 Releasing personal information to prevent or detect crime.....	24





2.3.7	Complaints .....	24
Part 3: Records Management Policy .....		24
3.1	Policy Statement .....	25
3.2	Scope .....	26
3.3	The Policy .....	26
3.3.1	Legislation .....	26
3.3.2	Records Creation.....	26
3.3.3	Records Classification.....	26
3.3.4	Metadata.....	27
3.3.5	Protective Marking.....	27
3.3.6	File naming .....	27
3.3.7	Record Storage, Security and Maintenance.....	27
3.3.7.1	Storage of physical records .....	27
3.3.7.2	Storage of electronic records.....	28
3.3.8	Version Control .....	28
3.3.9	Retention and Disposal of Records .....	28
3.3.10	Data Quality Assurance.....	29
3.3.11	Historical Records .....	30
Appendix 1 – Legal Requirements, Regulations and Standards .....		32
Appendix 2 - Related procedures and Guidance ( live document ) .....		33
Appendix 3 – Forum for Information Governance and Assurance.....		34
Appendix 4 – Glossary of Terms .....		36



## 1.0 Policy Statement

This Policy Framework consists of an Information Governance strategy and three Policies. The Information Governance strategy sets out the legal requirements which the Council is obliged to follow with regard to Information Governance (IG) and confirms the Council's commitments to these requirements. It also recognizes customers at the heart of Council business and brings together recognition of new ways of working and developing services to better meet customer need. This Policy also establishes a culture of individual responsibility for Information Governance, informed and supported by awareness and training for staff, Councillors and others working on behalf of the Council. This will enable all to understand the importance of information governance, know their responsibilities, and manage information appropriately.

This Policy Framework applies to all elected members, all staff and others working on behalf of the council i.e. partners, contractors and agents.

Non compliance with this framework and associated policies could potentially expose the council and/or its customers to unacceptable risk. Section 8 Governance and Compliance details responsibilities and consequences for non compliance applicable to all.

To this end, the Council commits to:

- **Information Governance Management:** Establishing and supporting robust operational and management accountability structures, with appropriate resources and expertise to ensure information governance 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:** Implementing a system of training and awareness that meets government mandatory requirements, is role based, assessed and capable of equipping employees with the skills and knowledge necessary to do their jobs and respond to customer demand.
- **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, policies and guidance documents in relation to the respective areas of information governance that support employees to fully understand the standards, practices and responsibilities required within the information governance framework and to take appropriate action where necessary.
- **Audit:** Monitoring employees' compliance with the information governance framework through regular audits.

The Information Governance Policy Framework (IGPF) is addressed in three parts:

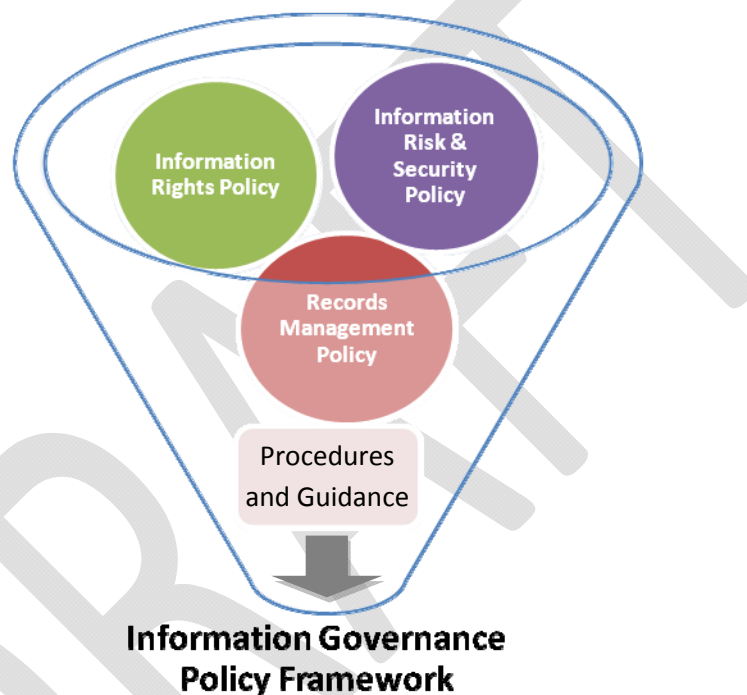
1. **Part 1: Information Risk & Security Policy** – including confidentiality, information sharing and privacy impact assessments.
2. **Part 2: Information Rights Policy** - including Freedom of Information, Environmental Information Regulations, and the Rights of Data Subjects under the Data Protection Act 1998 (subject access, objection to processing and amendments to inaccurate records).
3. **Part 3: Records Management Policy** – including Information Quality Assurance.



These Policies are intended to ensure that there is a robust framework concerning the obtaining, recording, holding, using, sharing and destruction of all data and records held or used by the Council and ensuring that relevant and accurate information is available where and when it is needed to improve service delivery to customers. It will also ensure that measures are in place to reduce the occurrence of breaches in information security.

This Policy Framework is owned by Head of Programme Delivery & Governance in the role of Senior Information Risk Owner (SIRO) and all existing procedures relating to Information Management, Information Security, Access to Information and Records Management will now fall under this framework

This framework will seek to bring together all of the existing procedures, requirements, standards and best practices and review/update them as appropriate.



A list of current procedures and guidance is contained within Appendix 2.

## 2.0 Purpose

The Information Governance arrangements will underpin the Council's strategic goals and ensure that the information needed to support and deliver their implementation is reliably available, accurate and understandable.

Information is a vital asset for the Council, supporting both day to day operations and the effective management of services and resources. Information is also important in regard to improvements to service delivery and how the Council is able to respond to changing customer needs and demands. Therefore it is essential that all Council information is managed effectively within a robust governance framework.

Successful application of this approach will lead to:

- Improvements in information handling activities.
- Reduction in numbers of IG incidents and complaints.
- Increased customer confidence in the Council and its staff.



### 3.0 What is Information Governance?

“Information Governance” describes the approach within which accountability, standards, policies and procedures are developed, implemented and maintained to ensure that all types of information used in the Council are sourced, held and used appropriately, securely and legally. Information Governance covers all information held by the Council (for example – staff, financial, estates, corporate, minutes) and all “information systems” used to hold that information. These systems may be purely paper- based or partially or totally electronic. The information concerned may be “owned” or required for use by the Council and hence may be internal or external.

As a provider of a range of services, the Council carries a responsibility for handling and protecting information of many types. These types of information include Personal data, commercially sensitive / confidential data and non – confidential / public data.

Having accurate relevant information available at the time and place where it is needed, is critical in all areas of the Council's business and plays a key part in corporate governance, strategic risk, service development and performance improvement and overall meeting the needs of our customers. It also supports a Council commitment to transparency and the Open Data agenda.

Good Information Governance will enable the Council to meet national requirements including annual submissions of the relevant Information Governance Toolkit. The Information Governance Toolkit is a performance tool, devised by Department of Health (Connecting for Health (2012) with the purpose of measuring an organizations compliance with national IG standards and relevant legislation).

The Council is obliged to abide by all relevant UK and European Union legislation. Appendix 1 contains a list of the some of the primary sources of legislation, standards and Guidance, relating to Information Governance with which the Council shall comply.

### 4.0 Applying the Policy Framework

In adopting this IGPF, the Council recognises and supports:

- The principle that accurate, timely and relevant information is essential to deliver high quality services and that it is the responsibility of all employees 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.
- The principles of corporate governance and public accountability places equal importance on the confidentiality of, and the security arrangements to safeguard, both personal information about customers, employees, and commercially sensitive information.
- The need to share customer information with partner organisations (particularly health and the third sector) and other agencies in a controlled manner consistent with the interests of the customer and, in some circumstances, the public interest.

### 5.0 Delivery

Through implementing these policies, the Council will:

- Establish robust information governance processes conforming to statutory requirements and national standards.
- Ensure that all practices and procedures relating to handling and holding personal and



Council corporate information are legal and confirm to best and / or recommended practice.

- Ensure that clear advice is given to customers about how their personal information is recorded, handled, stored and shared by the Council and its partners. Customers will be provided with guidance, available in various formats, to explain their rights, how their personal information is handled, how they can seek further information and how they can raise concerns.
- Ensure customer participation in IG developments, e.g. through the use of Privacy Impact Assessments.
- Provide clear advice and guidance to employees and ensure that they understand their responsibilities and apply the principles of Information Governance to their working practice in relation to protecting the confidentiality and security of personal information and appropriate handling of Council information assets.
- Maintain a clear reporting structure and ensure through management action and training that all employees understand IG requirements.
- Undertake regular reviews and audits of how information is recorded, held and used. Management Audits will be used to identify good practice and opportunities for improvement.
- Ensure procedures are reviewed to monitor their effectiveness so that improvements or deterioration in information handling standards can be recognised and addressed.
- Ensure that when service developments or modifications are undertaken, a review is undertaken of all aspects of information governance arrangements to ensure that they are robust and effective.
- Work to instil an Information Governance culture in the Council through increasing awareness and providing training on the key issues.
- Ensure there are robust procedures for notifying and learning from IG breaches and incidents in line with the Council's Information Risk and Security Policy.
- Assess its own performance using the Information Governance Toolkit and develop and implement action plans to ensure continued improvement.
- Ensure all new employees receive awareness training and information on information governance on an annual basis. The frequency and requirement of any further information risk and security training will be subject to the role and services delivered.

There are five interlinked principles which guide the application of this Information Governance Policy Framework:

- Quality Assurance
- Legal Compliance
- Information Security
- Proactive use of information
- Openness

To ensure **Information Quality Assurance**, the Council will:

- Establish, maintain and promote policies and procedures for information quality assurance and the effective management of records.
- Undertake or commission assessments and audits of its information quality and records management arrangements.
- Ensure that key customer data is accurately recorded and maintained, including regular cross-checking against source data.
- Ensure that managers / IAOs are required to take ownership of, and seek to improve the quality of information within their services and that information quality is assured at



the point of collection.

To ensure **Legal Compliance**, the Council will:

- Regard all identifiable personal information relating to customers and employees as confidential except where national requirements on accountability and openness require otherwise.
- Establish and maintain policies or procedures to ensure compliance with the Data Protection Act, Human Rights Act and the common law duty of confidentiality and all associated guidance.
- Establish and maintain policies or procedures for the controlled and appropriate sharing of service user information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act).

To ensure that appropriate and legal compliant **Information Security** exists, the Council will:

- Establish and maintain an Information Risk & Security Policy along with respective procedures for effective policing and secure management of all its Information Assets, resources and IT systems.
- Undertake and/or commission assessments and audits of its information and IT security arrangements in-line with the said policy.
- Promote effective confidentiality and security practices to ensure all permanent/temporary, contracted employees and third party associates of the Council adhere to this via appropriate laid down policy procedures, training and information awareness schemes/documentation.
- Establish and maintain appropriate policing, incident reporting procedures and monitoring and investigations of all instances, actual and/or potential, along with any reported breaches of confidentiality, security or the Data Protection Act.
- Identify and classify information to ensure that is handled and shared appropriately.

To ensure **proactive use of information**, the Council will:

- Ensure information systems hold the information required to support customer focused service delivery and operational management.
- Develop information systems and reporting processes which support effective performance management and monitoring.
- Develop information management awareness and training programmes to support managers in using information to manage and develop services.
- Ensure that, where appropriate and subject to confidentiality constraints, information is shared with other organisations in order to support improved service delivery.

To ensure **Openness**, the Council will:

- Ensure that non-confidential information about the Council and its services is readily and easily available through a variety of media, in line with the Council's FOI Publication Scheme.
- Implement policies to ensure compliance with the Freedom of Information Act and the Environmental Information Regulations.
- Ensure that customers have readily and easily available access to information relating to Council services, and their rights as service users.
- Have clear procedures and arrangements for liaison with the press and broadcasting media, and customers.



## 6.0 Information Governance roles and responsibilities

The Information Governance framework consists of a corporate forum FIGA (Forum for Information Governance & Assurance) which is accountable to the Corporate Management Team. Membership of the Forum will be Information Champions who hold senior roles in the Council and seek to Champion the principles and requirements of Information Governance across the Council. The board will be chaired by the SIRO and attended by the Information Governance Manager.

The Forum for Information Governance & Assurance (FIGA) is responsible for ensuring that risks are identified and addressed and providing assurance to the Chief Executive, Corporate Management Team and Members that the organisation takes information management and governance seriously and can demonstrate visible improvements through a risk-based approach. The Terms of Reference and membership are attached at Appendix 3.

Roles	Responsibilities
Senior Information Risk Owner (SIRO)	Is accountable for Information Governance, fosters a culture for protecting and using data, provides a focal point 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 organization. Provides a focal point for customer confidentiality & information sharing issues. Is concerned with the management of personal information
Data Protection Officer & Caldicott Advisor (Information Governance Manager)	The data protection function ensures that the Council has adopted good IG policies and procedures and complies with data protection laws. To coordinate data protection by design and privacy impact assessment initiatives and to be responsible for data security initiatives generally. This function will also act in an advisory capacity to the Caldicott Guardian where required. This function will be delivered through the role of the ' <b>Information Governance Manager</b> '
Information Risk & Security Officer	Responsible for developing, implementing and enforcing policies and procedures to protect information assets. This role also includes risk management and business continuity. Reporting to the Forum for Information Governance & Assurance on the information security status of the organisation by means of regular reports and presentation.
Records Officer	Responsible for developing, implementing and enforcing policies and procedures to ensure correct Information and Records Management practice across the council.
Information Champions	Champion awareness, understanding and compliance with the key principles of IG. Members of FIGA
Information Asset Owner	Designated senior officers with ownership and responsibility for specific information assets (paper based and electronic records, and IT systems). Supported by <b>Information Asset Custodians</b>

Information Asset Custodian	Designated officer with responsibility for daily management and protection of specified Information Assets. (paper based records and IT systems)
-----------------------------	--

## 7.0 Strategy implementation

The FIGA will monitor implementation of this strategy and its associated work programmes through regular meetings and activities carried out by the Information Governance Team. This will involve:

- Conducting a baseline assessment of the current position in relation to IG standards (Using the self assessment toolkit).
- Agreeing an annual work programme to ensure year on year improvement in performance.
- Ensure the development of strategies, policies, procedures etc required for information Governance.
- Identify resources required for implementation.
- Report on progress, incidents and issues to CMT / Members.

The FIGA will review this strategy annually or in response to any significant changes to mandatory requirements, national guidance or as a result of significant information governance breaches or incidents.

Information Asset Owners will be key as officers accountable and responsible for Information Assets across the Council and ensuring that appropriate IG arrangements are in place.

## 8.0 Governance and compliance

Non-compliance with this Framework and relevant policies could potentially expose the council and /or its customers to risk.

### 8.1 Employees

All new and existing employees ( including school – based staff) will receive awareness training and guidance on Information Governance, which will include Confidentiality, Data Protection, Information Security and Information Rights procedures. Employees who do not comply with these policies may therefore be subject to Disciplinary action, in line with the Councils Disciplinary Procedures.

### 8.2 Elected Members/Councillors

All elected members will receive awareness training and guidance on Information Governance, which will include Confidentiality, Data Protection, Information Security and Information Rights procedures. Members' failure to comply with these policies will constitute a potential breach of the Council's Member's Code of Conduct and associated Member/Officer Protocol. Breaches of the Member's Code of Conduct may be subject to Sanction imposed by the Standards Committee.





### 8.3 Others working on behalf of the council

All partners, contractors and agents of the council, should be appropriately trained in respect of Information Governance, including Confidentiality, Data Protection, Information Security and Information Rights procedures. Employees who do not comply with these policies may therefore be subject to Disciplinary action, in line with the Councils Disciplinary Procedures.

### 8.3 Responsibilities

The Information Governance Manager shall be responsible for managing and implementing the policies and related procedures on a day-to-day basis.

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

- read and understood the policies applicable in their work areas
- been made aware of personal responsibilities for the policies
- access advice on the policies
- Received appropriate and up-to-date training relating to Information Governance.

Non -compliance with the policies could potentially expose the council and /or its customers to risk. Employees who do not comply may therefore be subject to action under the Councils Disciplinary Procedures

The following table identifies who within Walsall Council is Accountable, Responsible, Informed or Consulted with regards to these policies. The following definitions apply;

- **Accountable** – the person who has ultimate accountability and authority for the policies.
- **Responsible** – the person(s) responsible for developing and implementing the policies.
- **Consulted** – the person(s) or groups to be consulted prior to final policy implementation or amendment.
- **Informed** – the person(s) or groups to be informed after policy implementation or amendment.

<b>Accountable</b>	Senior Information Risk Owner
<b>Responsible</b>	Information Governance Manager
<b>Consulted</b>	CMT / Forum for Information Governance & Assurance
<b>Informed</b>	All Council Employees, Elected Members and Partners



# Part 1: Information Risk and Security Policy

## 1.1 Policy Statement

Information is a vital asset to the organisation, Walsall Council (the Council) is committed to preserving the confidentiality, integrity, and availability of our information assets:

- For sound decision making;
- To deliver quality services;
- To comply with the law;
- To meet the expectations and demands of our customers;
- To protect our reputation as a professional and trustworthy organisation.

The purpose of the Information Risk & Security Policy is to protect the Council's information, manage information risk and reduce it to an acceptable level, while facilitating reasonable use of information in supporting, customer demand and normal business activity for the Council and its partners.

This will be achieved through establishing and maintaining the security and confidentiality of information, information systems, applications and networks owned or held by the Council.

**Customer Voice: "Please help me by keeping all information you have about me safe and secure"**

The Information risk and security management Policy will ensure an appropriate level of:

**Integrity** All information assets and system are operating according to specification and the accuracy of data is maintained.

**Security** Information is obtained, held and disclosed lawfully and data access is confined to those with specified authority to view and/or change the data.

**Availability** Systems and data are available when required and the output from it delivered to the user or customer who needs it, when it is needed.

This will be achieved by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this and other policies.
- Describing the principles of security and explaining how they shall be implemented in the organisation.
- Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- Creating and maintaining within the organisation a level of awareness of the need for Information Security as an integral part of the day to day business.



## 1.2 Scope

This policy applies to all councillors, employees, partners, contractors and agents of the Council (i.e. users) who use or have access to council information assets, computer equipment or ICT facilities.

The policy applies throughout the lifecycle of the information from creation, storage, and use to disposal. It applies to all information including:

- Information stored electronically on databases or applications e.g. email;
- Information stored on computers, PDAs, mobile phones, printers, or removable media such as hard disks, CD Rom, memory sticks, tapes and other similar media;
- Information transmitted on networks;
- Information sent by fax or other communications method;
- All paper records;
- Microfiche, visual and photographic materials including slides and CCTV;
- Spoken, including face-to-face, voicemail and recorded conversation.

## 1.3 The Policy

### 1.3.1 Information Assets & Risk Management

A risk assessment will be carried out for each of the Council's information Assets in all formats and mediums and measures put in place to ensure each Asset / system is secured to an appropriate level. This process will involve identifying threats and vulnerabilities (severity of impact and the likelihood of occurrence) at an individual asset level and, from there, analysing and assessing risks in order to make the best use of resources, each Information Asset will be secured to a level appropriate to the measure of risk associated with it.

Information Security risks shall be recorded within a baseline risk register and action plans shall be put in place to effectively manage those risks. The risk register and all associated actions shall be reviewed at regular intervals. Any implemented information security arrangements shall also be a regularly reviewed feature of the Council's risk corporate management programme.

### 1.3.2 Information Asset Security & Confidentiality

Information risk and security management controls and procedures for all Information Assets will conform to the International Standards for Information Security ISO27001:2005 and ISO27002.

The security of all information assets must be considered at all stages of the asset lifecycle. The risks associated with handling, storing and sending information must be identified and mitigated, giving due regard to the Common Law Duty of Confidentiality. Processes for handling Information Assets must give regard to relevant statutory and regulatory requirements.

The ICT Systems and Infrastructure will be designed wherever possible to provide maximum availability that backups are taken and individual disaster recovery plans exist for key systems. The following bullet points briefly cover the key guidelines for the existing systems and for introducing new systems and infrastructure:



- Appropriate measures are taken to protect the Councils information and systems from damage or loss due to malicious software such as viruses.
- The availability of information is maintained, i.e. by ensuring that information and information systems are available to authorised users when required.
- Business continuity plans are produced, maintained and tested.
- A consistent system for the classification of information assets within the Council.
- Robust Password and Access Control.

### 1.3.3 Information Sharing

**Customer Voice: “Help me by sharing my information when and with who you are supposed to help make services better for me”**

This Policy supports effective and appropriate information sharing across the council and with partner organisations as part of overall service improvement. Sharing of information with partners and organisations is subject to the Protocol for Information Sharing. Information sharing with external organizations should be supported by a purpose specific information sharing agreements. Sharing of information within the Council may also need to be supported by a robust Information Sharing Agreement. All agreements should be made in consultation with the Information Governance Team and signed by the relevant Information Asset Owner(s). Approval should also be sought from the SIRO and / or Caldicott Guardian where appropriate.

### 1.3.4 Systems Development, Planning and Procurement

Security and risk management issues must be considered and documented during the requirements phase and the procurement phase of all system procurements and developments. Minimum security standards and information governance requirements will be incorporated in all new systems.

### 1.3.5 Contracts

Contracts with external contractors that allow access to the organisation’s information systems shall be in operation before access is allowed. These contracts shall ensure that the staff or sub-contractors of the external organisation shall comply with all appropriate security policies and procedures.

### 1.3.6 Contracts of Employment

Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause. Information security expectations of staff shall be included within appropriate job descriptions.

### 1.3.7 Business Continuity Planning

All systems and Information Assets will have threats and vulnerabilities assessed to determine how critical they are to the Council. Individual departments should have procedures in place to maintain essential services in the event of IT system failure or the loss of primary Information Assets held in other formats.

### 1.3.8 Intellectual Property Rights

The Council will ensure that all information products are properly licensed and approved by the Information Risk and Security Officer. Users shall not install software on the Council’s property without permission from the lead officer responsible for Information Risk & Security. Users breaching this requirement may be subject to disciplinary action.



### **1.3.9 Personal Use**

Personal use of Council ICT equipment is permitted providing that it is in line with the provisions of the Email and Internet Usage Policy and Procedures and other related procedures relating to the use of these devices.

### **1.3.10 Breach Management**

The Council's Breach Management procedure must be followed wherever there is any unauthorised or unlawful disclosure, loss, damage or destruction to personal or confidential information. All staff should be made aware of the procedure and the reporting requirements.

DRAFT



# Part 2: Information Rights Policy

## 2.1 Policy Statement

Walsall Council is fully committed to transparency, whilst recognising the need for an appropriate balance between openness and maintaining the security and (where necessary) the confidentiality of the information which it holds. It uses an assumption of full disclosure as a starting point for considering all requests for information. Information will only be withheld where there is a genuine and justifiable reason for doing so that can be supported by legislation.

Walsall Council also recognises the rights of individuals in respect of information the Authority holds about them. These rights are;

- A right of access to a copy of the information comprising of their personal data;
- A right to object to processing that is likely to cause or is causing damage or distress;
- A right to prevent processing for direct marketing;
- A right to object to decisions being taken by automated means;
- A right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed; and
- A right to claim compensation for damages caused by a breach of the Data Protection Act.

From a customer perspective, this policy seeks to ensure they are able to get the information they are entitled to and that personal information about them is used in accordance with their rights and wishes.

## 2.2 Scope

This policy relates to all services of Walsall Council and all information created and received by Walsall Council, regardless of media or format. This includes all paper-based records as well as information that exists, or will exist, solely in electronic form, audio/visual records and photographs.

## 2.3 The Policy

### 2.3.1 Freedom of Information (FOI)/Environmental Information Regulations (EIR)

**Customer Voice: "Help me find out what I want to know"**

#### 2.3.1.1 Making a request

To be valid FOI or EIR, requests;



- Must be in writing and be legible – FOI only
- Can be oral or legible when written - EIR
- Must clearly describe the information being sought;
- Can be made by an individual or an organisation;
- Must contain a name and a return address (this does not need to be a postal address but could be, for example, an email) and
- Can be sent to / received by any part of the organisation

To be valid EIR/FOI requests they **do not**;

- Have to be written in a special form;
- Need to mention the FOI Act; or need to refer to “Freedom of Information”.
- Need to mention the EIR; or need to refer to the “Environmental Information Regulations”.
- Need to have been received directly to the Information Governance Team

### 2.3.1.2 Environmental Information Regulations

#### Definition

Environmental Information Regulations (EIR) cover the following information;

1. The state of the elements of the environment, such as air and atmosphere, water, soil, land, landscape and natural sites including wetlands, coastal and marine areas, biological diversity and its components, including genetically modified organisms, and the interaction among these elements;
2. Factors, such as substances, energy, noise, radiation or waste, including radioactive waste, emissions, discharges and other releases into the environment, affecting or likely to affect the elements of the environment referred to in (a);
3. Measures (including administrative measures), such as policies, legislation, plans, programmes, environmental agreements, and activities affecting or likely to affect the elements and factors referred to in (a) and (b) as well as measures or activities designed to protect those elements;
4. Reports on the implementation of environmental legislation;
5. Cost-benefit and other economic analyses and assumptions used within the framework of the measures and activities referred to in (c); and
6. The state of human health and safety, including the contamination of the food chain, where relevant, conditions of human life, cultural sites and built



structures inasmuch as they are or may be affected by the state of the elements of the environment referred to in (a) or, through those elements, by any of the matters referred to in (b) and (c).

The Council recognises that there are many similarities between the two regimes and that requests for “environmental Information” must be answered in accordance with the EIRs rather than the FOI Act. Request under the Environmental Information Regulations will be handled in the same way as those under FOI, with due reference to the provisions of those Regulations.

It is possible that in some cases both regimes will be relevant. The Council will, when responding to such requests for information, endeavour to clearly identify which parts of the information fall under which regime. The Council will also seek to ensure that where requests for information are made and form part of everyday service delivery they are treated as ‘business as usual’ and not considered as valid requests under the EIR /FOI Act.

#### 2.3.1.3 Advice and assistance

The Council has a duty to provide advice and assistance to applicants under Section 16 of the FOI Act so far as it would be reasonable to expect the Authority to do so. The Council will offer advice and assistance to any person or organisation that wishes to make a request for information.

#### 2.3.1.4 Handling Requests

All valid FOI/EIR requests will be handled by the Information Governance Team. Where a valid FOI/EIR request is received directly by a service it should be forwarded immediately to that team for processing. This does not preclude officers from dealing with day to day enquires or providing customers with information as part of ‘business as usual’.

#### 2.3.1.5 Timing of Requests

All requests will be responded to as promptly as possible, and in any event no later than 20 working days. The requester should be kept informed of any delays.

#### 2.3.1.6 Refusing a request

The Council uses the presumption of release as the starting point for all information requests. The Council recognises that there will always be some information which it must not disclose or which it is not in the public interest to disclose. In the case where the Council refuses to disclose information and therefore relies upon a Exemption / Exception the Council will ensure that applicants are given clear and accurate written reasons for the refusal of their requests and assistance where appropriate. If the reasoning behind the refusal or the refusal itself, would result in the disclosure of information which would itself be exempt, then the Council may not provide that reason.

Applicants have the right to have a decision to refuse the disclosure of information reviewed. Applicants will be informed of this right and may seek such a review if dissatisfied with the Council’s response.

If the Council decides that the public interest in maintaining the exemption outweighs the public interests in disclosure, then this will be stated in the refusal letter together with the public interest factors, which have been considered, and





which form a material part of the decision.

If a document contains exempt information, the Council will not refuse access to the whole document unless it is absolutely necessary to do so in order to ensure that exempt information is not disclosed. Where part of a document is exempt, normally only that part of the document containing the exempt information will be withheld.

In accordance with the Freedom of Information and Data Protection (appropriate Limits and Fees) Regulations 2004, the Council is not obliged to respond to a written request for information, where it estimates that the cost of complying with the request would be in excess of £450 (which equates to 18 hours of work at £25 per hour). If it is believed that a request is likely to exceed this limit, the Council will explain clearly to the requester how this estimate has been arrived at and offer them assistance in refining their request in order to bring it to within the appropriate limit.

#### 2.3.1.7 Qualified Person

The Head of Legal and Democratic Services is authorised to act as the “qualified person” under Section 36 of the FOI Act (This function cannot be delegated).

#### 2.3.1.8 Consultation with third parties

The Council recognises that disclosure of information may affect the legal rights of a third party and this policy is written in accordance with the terms of the Data Protection Act 1998 and the Human Rights Act 1998. The Council further recognises that unless an exemption / exception is provided for in the FOI Act / EIR there will be a requirement to disclose that information in response to a request.

If the consultation with a third party is required prior to disclosure of information, the Council will, seek to do so, at the earliest opportunity, with a view to seeking their views on disclosure, unless such a consultation is not practical. If the cost of consultation with the third party is disproportionate, consultation may not be undertaken. The consultation may assist the Council in determining whether an exemption under the FOI Act / EIR applies to the information requested, or the views of the third party may assist the Council in determining where the public interest lies. A third party's unwillingness to agree with disclosure of information does not necessarily mean that information will not be disclosed. The Council will not undertake consultation if it does not intend to disclose the information because it has already determined that valid exemption/ exception.

#### 2.3.1.9 Contracts

The Council will not enter into any contracts which purport to restrict the disclosure of information held by the Council in relation to the contract beyond valid exemptions / exceptions.

#### 2.3.1.10 Repeat requests

Where a repeated request is received that is identical or substantially similar to a previous request from the same person, the Council will consider this as a repeated request. The Council is not obliged to comply with repeat requests for information. Any decision not to respond to a repeat request must be made in consultation with the Information Governance Manager.

Where a requester is considered unreasonable or unreasonably persistent, the



Council's Unreasonable and Unreasonably Persistent Complaints procedure will be adhered to.

#### 2.3.1.11 Publication scheme

The Council has adopted a Publication Scheme and is committed to updating and maintaining it to keep it current and relevant. The Publication Scheme contains documents, policies, plans and guidance used by the Council. The material contained within the Scheme is available on the Internet. Where charges are applied these will be stated in the Scheme.

### 2.3.2 Subject Access Requests

#### **Customer Voice: "Help me find out what the Council knows about me"**

To be a valid subject access request under the Data Protection Act (DPA), requests;

- Must be in writing and be legible
- Must contain enough detail to be able to locate the required information;
- Must be made by the data subject or someone authorised to act on their behalf and
- Can be sent to /received by any part of the organisation

To be valid under the DPA requests **do not**;

- Have to be submitted on a specific form;
- Need to mention the DPA Act or the term 'subject access'; or
- Need to have been received directly by the Information Governance team

#### 2.3.2.1 Confirming Identity

The Council will take reasonable steps to confirm the identity of the requester. However the Council will not make this identification process unnecessarily onerous and in cases where the requester is already well known to the Council (e.g. an existing member of staff or a social services client with an active social worker) formal identification will not be sought.

#### 2.3.2.2 Handling Requests

All requests will be handled by the Information Governance Team, where a valid request is received under the DPA, directly by a service or member of staff, it should be forwarded immediately to that team for processing. This does not preclude officers from dealing with day to day enquires or providing 'data subjects' with their own information as part of 'business as usual'.

#### 2.3.2.3 Timing of Requests

All requests will be responded to as promptly as possible, and in any event no later than 40 calendar days. The requestor should be kept informed of any delays.



#### 2.3.2.4 Access to Personal Data by an authorised / legal agent

When an agent makes a request on behalf of a Data Subject, signed authorisation from the Data Subject will be required. The Council may still check directly with the Data Subject whether he or she is happy with the agent receiving the personal data and should highlight the implications of the request.

Any request received from an agent must be accompanied by signed Form of Authority [permission] from the Data Subject. No proof of identity for a Data Subject is required when the application comes from a professionally recognised agent such as a Solicitor

#### 2.3.2.5 Access to Personal Data of a Child

A parent or guardian may access personal data on behalf of their child if the child is considered to be unable to submit a request. The Council is aware that in some cases it might not be appropriate to release the child's information to the parents. The safety and wellbeing of the child will be the key determining factor in whether or not information can be disclosed. See 'Dealing with Subject Access Requests (SARs) Procedure'

#### 2.3.2.6 The Mental Capacity Act

Subject Access requests made on behalf of individuals that do not have adequate mental capacity can be made by those appointed to act on his/her behalf under Lasting Power of Attorney or by the Court of Protection. The Council will ensure that the best interests of the data subject are always considered.

#### 2.3.2.7 Information containing third party data

The Council may refuse a subject access request where releasing that information would also involve disclosing information about another individual, except in cases where;

- That individual has consented to disclosure; or
- It is reasonable in all the circumstances to comply with the request without that individual's consent.

The Council will seek to balance the rights of the requester with the rights of the third party and only release information if, in all circumstances, it is reasonable to do so.

#### 2.3.2.8 Access to records of deceased individuals

The Data Protection Act only relates to living individuals; however the Council recognises there is still a common law duty of confidentiality owed to the records of deceased individuals. The Council will act in the best interests of the estate.

#### 2.3.2.9 Refusing a request

The Council uses the presumption of release as the starting point for all valid subject access requests. Where there is a legitimate reason why information should not be disclosed (e.g. the prevention or detection of crime) the applicant will be informed of the reasons why and of their right to appeal.



### 2.3.3 Privacy Notices

**Customer Voice: "Help me understand how you will use my information"**

The Council will issue a privacy notice wherever it is collecting personal data. The content of the privacy notice will vary depending on what is being collected and for what purpose, but as a minimum should include;

- The Council's identity
- The purpose or purposes for which the information is being collected
- If the information will be shared and if so who with
- Contact details for the Council's Data Protection Officer

### 2.3.4 Amendments to inaccurate records

**Customer Voice: "Help me to make sure the Council is making decisions about me based on the right facts"**

The Council acknowledges the individual's right to challenge the accuracy of the personal data held about them where they believe it to be inaccurate or misleading.

Where information is found to be factually inaccurate it will be updated immediately, where there is dispute between the Council and the data subject as to the accuracy of information, a note will be made on the record to that effect and both sets of information will be kept on the file.

### 2.3.5 Objections to Processing

Individuals have the right to;

- Prevent the processing of data which is likely to cause them substantial damage or substantial distress.
- Prevent processing for the purposes of direct marketing.

#### 2.3.5.1 Direct Marketing

**Customer Voice: "Don't send marketing to me when I don't want it"**

The Council will maintain a register of all requests to prevent an individual's information being used for the purposes of direct marketing. Where any marketing exercise is considered, the responsible officer should consult with the Information Governance team to cross reference this register and will not contact anyone who has submitted such a request.

Requests to prevent processing for direct marketing must be in writing.

#### 2.3.5.2 Prevention of processing likely to cause substantial damage or distress

**Customer Voice: "Don't use information about me if this harms me"**

An individual who wants to exercise this right is required to put their objection in writing to the Council and state what they require the Council to do to avoid causing damage or distress. An individual can only object to the processing of their own



personal data and the objection must specify why the processing is causing unwarranted and substantial damage or distress.

The Council will only stop processing personal information where it is found to be causing unwarranted and substantial damage or distress.

All requests to prevent processing will be responded to within 21 days, stating if the Council intends to comply with the request either in whole or in part and, where necessary, stating the reasons why the request will not be complied with.

### 2.3.6 Releasing personal information to prevent or detect crime

#### **Customer Voice: "Help the police and other law enforcement agencies protect me from crime"**

It is Council policy to cooperate wherever possible with requests for personal information for the prevention or detection of crime or identification or apprehension of suspects, but only after satisfactory checks have been completed to protect the rights of data subjects. Information will only be released where disclosure meets the criteria outlined in Section 29 of the Data Protection Act 1998

Requests under s29 will only be considered from an agency with a crime or law enforcement function, including the Police, HMRC, The UK Border Agency, or the Benefit Fraud sections of DWP or other Local Authorities.

Requests must be in writing and be clear on what is being asked for and why the release of the information is critical to the investigation.

Only information directly relevant to the purpose stated will be released, and only the minimal possible to enable the law enforcement agency to do their job. The transfer of information will be via a secure channel (e.g. secure email or special delivery post.)

### 2.3.7 Complaints

The Council has an Appeal Procedure for dealing with complaints made in relation to requests under FOI, EIR or DPA. Any person who is unhappy with the way in which the Council has handled their request may use this procedure. The Information Commissioner is unlikely to investigate any complaint about the Council's handling of an information request unless the complaints procedure has been exhausted.

Appeals will be heard by an officer(s) not involved in the original decision.

A complaint may be made about the Council's failure to release information in accordance with its Publication Scheme, failure to comply with an objection to processing or to amend inaccurate records. Complaints can also be made about requests that have not been properly handled, or where there is dissatisfaction with the outcome of a request.

## Part 3: Records Management Policy



### 3.1 Policy Statement

Walsall Metropolitan Borough Council recognises that its **records** are an important corporate and public asset, and are a key resource in the council's effective operation and accountability. They also provide a history of the borough and its democratic processes.

It is the policy of Walsall MBC that "authentic, reliable and useable records are created which are capable of supporting business activities and functions for as long as they are required" (ISO 15489-1 2002 Clause 6.2).

As with any other asset, records require careful management from creation to ultimate disposal. It is recognised that there are risks associated with the handling of records and information in order to conduct official Council business and this policy aims to mitigate these risks. This includes:

- Failure to correctly manage corporate records
- Inadequate destruction of data
- Premature or delayed destruction of data (failure to apply correct retention periods)
- Incorrect handling of records classified as PROTECT, RESTRICTED or CONFIDENTIAL
- Poor business decisions based on inadequate or incorrect information
- Potential sanctions against the Council or individual officers imposed by the Information Commissioner's Office as a result of the misuse, loss or unauthorised / malicious destruction of City Council records.
- Damage to the Council's reputation as a result of information loss or misuse.

This policy sets out the council's responsibilities and activities in regard to Records Management. It provides the framework for more specific departmental and service guidance and detailed operating procedures.

The policy describes how the Council will:

- Establish the rules and standards for classifying, referencing, titling, indexing and protectively marking records to enable the efficient retrieval of information;
- Comply with legislation to protect the Council, or any of its staff, or elected members from risk of contempt of court or other legal proceedings;
- Support the decision-making processes with clear, accurate, and relevant evidence;
- Ensure that adequate and appropriate storage is provided for all records, that they remain safe from unauthorised access and that disaster recovery policy and procedures are in place;
- Ensure that where a system is in place it is understood by appropriate staff with access to relevant training;

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



## 3.2 Scope

The policy covers the management of *all* records of the Council regardless of medium or format, including electronic records and it is applicable to all employees of the Council who use or create records for the Council as well as Elected Members, volunteers, consultants and partner organisations.

## 3.3 The Policy

**Customer Voice: “Help me by making best use of my information and sharing it appropriately so that I only have to give it to you once”**

Walsall Council holds a vast number of records that are important sources of information and are either vital to the operation of the Council or form an invaluable historical context. Management of these records is a discipline that should control all aspects of the record life cycle from its creation through to appropriate disposal.

### 3.3.1 Legislation

Most functions within the Council, both statutory and non-statutory, operate within specific legislative frameworks that may govern the creation, use, storage and disposal of records. There are however a number of key pieces of legislation that require access to, and/or effective management of, Council records, these are detailed in: *Information Governance Appendix 1 – Legal Requirements, Regulations and Standards*.

### 3.3.2 Records Creation

The creation of records is a recognised part of the lifecycle of a record. All council records are subject to all parts of this policy from the point of creation, and should be captured into an appropriate storage system and have a review/destruction date applied from this point.

### 3.3.3 Records Classification

In order to facilitate the effective storage, management and sharing (where appropriate) of council information, and to enable information stored in different formats to be easily ‘linked’ and cross referenced, records should be classified and arranged in a logical and consistent manner. To this end, departments should use the Local Government Classification Scheme (LGCS) and supporting guidance issued by the Council to classify all records regardless of format.

The structure of the LGCS works from the most general description or Function, at the first level, down to a more specific description, or Transaction, at the lower levels

Items stored on Walsall Councils IT servers (commonly known as shared drives) should be arranged in a file structure based on the LGCS format.

To facilitate ease of retrieval, and help prevent the loss of information, file tracking systems for paper records must be put in place, where they do not already exist.

It is the responsibility of the Records Officer to provide guidance and support on the LGCS, file structures and file tracking systems.



### 3.3.4 Metadata

Metadata is used to describe a record, its relationships with other records, and any access and retention requirements placed on it. Metadata allows users to locate and evaluate data quickly and effectively. A structured format allows for a precise description of content, location, and other key elements.

Metadata should be assigned to each record or collection of records. Metadata elements must be selected from the **e-GMS** or other approved standard and, at the very least, will include: The Creator, Date Created, Description, Title, Protective Marking, and a Disposal / Review Date

### 3.3.5 Protective Marking

A protective marking scheme is a set of rules employed to define the security qualities of different types of information. It allows a clear set of guidelines to be developed covering use, access and protection of that information.

All records and information created, received, communicated, or stored by the council need to be classified either at the point of creation or receipt, and to carry that classification as a discrete marker. A report may have a header of 'confidential' or a group email may carry a header of 'restricted'. In practice 'public' or unclassified information does not need to be marked.

Further guidance on the application of protective markers can be found in the Information Rights Policy, and the Protective Marking Procedure.

### 3.3.6 File naming

Records should be described/named in a logical, consistent, and predictable way to ensure fast, accurate and comprehensive retrieval. They should be given meaningful names that reflect their content.

Where records have elements in both physical and electronic format they should be named consistently to enable cross referencing. Detailed guidance in respect of file naming can be found in the appropriate Records Management Procedure.

### 3.3.7 Record Storage, Security and Maintenance

All records, manual or electronic, will be stored in such a way as to enable them to be:

- protected from unauthorised access;
- located and accessed when necessary;
- destroyed/disposed of appropriately when necessary;
- protected against accidental loss or destruction;
- protected from damage, be it accidental, malicious or environmental

#### 3.3.7.1 Storage of physical records

Storage accommodation for physical records should be clean and tidy in order to prevent damage to the records. Locations used for the storage of current records should be safe from unauthorised access while allowing maximum accessibility to the information commensurate with its frequency of use.





Records storage facilities, shelving and equipment must meet occupational health and safety requirements.

Records that are no longer needed onsite but are still required to be retained by the council should be sent to the council's preferred corporate contractor for offsite storage.

Departments must consult with the Records Officer on the long-term storage or archiving of paper records and must, on no account, make separate arrangements.

### 3.3.7.2 Storage of electronic records

Records stored in an electronic format should be treated with the same consideration for security and access.

Ideally, the format of electronic records should be consistent to allow exchange across systems to be facilitated where appropriate. Every effort will be made to cross reference electronic records with any corresponding paper records where possible, with appropriate indexing and classification.

Where information has been electronically captured by scanning, compliance with BIP0008:2004 is essential. It is the responsibility of the Records Officer to provide advice and support on compliance with BIP0008 2004. Please see: Information Governance - *Appendix 1 – Legal Requirements, Regulations and Standards* for more details

**Any records that could potentially be used as evidence in a legal or regulatory process should be subject to access and audit trail controls to ensure that their reliability, integrity and evidential value could be demonstrated, if required.**

Records stored electronically are subject to the same retention requirements as paper based records. Failure to apply destruction/review dates to electronic information can lead to potential breaches of legislation as well as increased usage of server space.

Arrangements will be put in place to maintain record integrity regardless of format; these will be described in the associated Data Quality procedure.

### 3.3.8 Version Control

In order to track changes to documents and ensure the most recent version can be identified then a version control table which tracks previous version numbers should be included in the document.

This should indicate the date of any changes with a version number, as will help keep track of the most up-to-date version. If more than one person is working on a record it is important to indicate who made what changes, on what date and in what specific areas.

### 3.3.9 Retention and Disposal of Records

**Customer Voice: "Help me by disposing of my information safely and securely so it doesn't end up in the wrong hands"**



The council will create, update and maintain a comprehensive Retention Schedule, to provide clear guidance on how long records should be kept for. This guidance will be applicable to all records, regardless of format.

This document considers detailed business processes and the legislative and operational environments within each function.

The latest version will always be available on the Council Intranet. It will be the responsibility of the Records Officer supported by Information Asset Owners to ensure that the Retention Schedule remains in line with all appropriate legislation. It shall be reviewed and updated where necessary no less than once a year.

Records identified for disposal in accordance with the schedule and other relevant guidelines will be disposed of by a method appropriate to the level of confidentiality of the record and in accordance with any attached security labels.

Confidential or sensitive records should be destroyed in a secure manner, with details kept of the reference, description, and date of destruction. These details should show what records are designated for destruction, the authority under which they are to be destroyed and provide background information on the records, such as legislative provisions, functional context and physical arrangements.

In the event that a record due for destruction becomes the subject of a request for information, under the Freedom of Information Act, then destruction will be delayed until the request has been satisfied or, in the case of a refusal to provide the information, until any complaint/appeal mechanism has run its course. Before a formal request for information has been received, amendments or deletion can take place in line with council policy and procedure.

### 3.3.10 Data Quality Assurance

**Customer Voice: "Help me by keeping my information accurate and up to date, so that I get the services that are right for me"**

Walsall Council has a responsibility to ensure that the information it uses to carry out business functions is correct and fit for purpose, and remains so for as long as it is required to be retained.

Walsall Council is committed to the application of the six dimensions of data quality: **accuracy, validity, reliability, timeliness, relevance, and completeness.**

All staff have a duty to manage information in their service area in such a way as to ensure it is collected, managed and used appropriately, and to make certain that it is complete, accurate and inspires confidence in users.

Where records contain personal information the fourth principle of the Data Protection Act (1998) stipulates that this data is captured and retained accurate and up to date. All staff collecting or using personal data have a responsibility to ensure that this is the case.

It will be the responsibility of the Records Officer supported by Information Asset Owners/Heads of service to ensure that staff are trained in records creation, use



and maintenance, and to provide ongoing data quality support and guidance.

### 3.3.11 Historical Records

Walsall Council aims to protect records that are considered to have unlimited and permanent value for legal, administrative, or research purposes.

The council's retention schedule will indicate records that are of potential historical significance. It is the responsibility of Information Asset Owners and Information Asset Custodians to contact the Local History Centre regarding records of this type, where they no longer of active or administrative use.

Further Information on the appropriate use of the councils archives serve can be found in the Archive Procedures.

DRAFT

**Version History**

Revision Date	Version	Revised By	Summary of Changes
18/12/12	V 0.1	N Ukaidi - Principal Performance Officer (Information & Records ) James Sparrock – Records Officer	Creating of consolidated Information Governance Policy Framework document comprising three polices (associated formatting and contextual changes)
20/12/12	V 0.2	N Ukaidi - Principal Performance Officer (Information & Records) James Sparrock – Records Officer	Incorporating comments and amendments received from Corporate Management Team
07/02/13	V0.3	N Ukaidi - Principal Performance Officer (Information & Records)	Incorporating comments and amendments received from Employee Relations Forum

**Approvals**

This individual Framework and Policies received the following approvals.

Name	Title	Signature	Date of Approval
P. Gordon	Assistant Director (Resources)		27/11/12
C. Williams	Senior Information Risk Owner		23/11/12
M. Sadler	Head of Procurement & Shared Services		
Suzanne Joyner	Caldicott Guardian		29/11/12
FIGA – Forum for Information Governance & Assurance			7/12/12

The consolidated IG Policy Framework requires the following approvals.

Name	Title	Signature	Date of Approval
CMT – Corporate Management Team			
Elected Members - Full Cabinet			



## Appendix 1 – Legal Requirements, Regulations and Standards

The Council and all its employees are governed by a number of laws, regulations and standards relating to Information Governance, these include:

- Data Protection Act 1998
- The Data Protection (Processing of Sensitive Personal Data) Order 2000
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Access to Medical Records Act 1991
- Report on the Review of Patient - Identifiable Information (Caldicott Report) December 1997.
- Human Rights Act 1998
- Civil Evidence Act 1995
- Regulation of Investigatory Powers Act 2000
- Local Government Act 1972 (Section 224)
- NHS Confidentiality Code of Practice 2003
- International Standards for Information Security - ISO27001:2005  
- ISO27002
- International Standard for Information and Documentation, Records Management
- ISO 15489
- Information technology; Code of practice for information security management  
ISO/IEC 17799
- Code of practice for legal admissibility and evidential weight of information stored electronically BIP0008:2004



## Appendix 2 - Related procedures and Guidance (live document)

- Breach Management Procedure
- Use of Removable Media Procedure
- Dealing with Subject Access Requests (SARs) Procedure
- Data Quality Procedure
- Version Control Procedure
- Records Storage Procedure
- Archive Procedure
- Naming Convention Procedure
- Information Security Procedures
- E-mail & Internet Usage Procedure
- Handling Person Identifiable Data

DRAFT



## Appendix 3 – Forum for Information Governance and Assurance

### Terms of Reference for Forum for Information Governance & Assurance

#### Purpose

*To keep information assets safe: capture the information we need, store it appropriately, use it wisely and effectively and then destroy it safely.*

#### Key Activities

- Provide assurance to the Chief Executive and Corporate Management Team that the organisation has taken information management seriously, can demonstrate visible improvements and is addressing issues on a risk-based approach.
- Encourage openness and sharing of good practice and learning.
- Own the overall Policy for: Information Governance, Security, DPA Compliance, Assurance, Records Management and Sharing ensuring they are fit for purpose.
- Monitor the effectiveness of information management training and its take up.
- Approve changes to policies and procedures relating to Information Assurance.
- Monitor the effectiveness of the Council's process for handling investigations and reporting incidents and breaches.
- Quality assure the work of the Information Management project and the Information Management / Governance Team beyond the life of the project.

#### Accountability

This board will report to the Chief Executive and Corporate Management Team through the Senior Information Risk Owner.

#### Meetings

The group will meet quarterly. Deputies are not required. Decisions may be made outside of the physical board meeting via email confirmation.



Information Champions may choose to have their own directorate Asset Owners meetings which may feed agenda items into this board.

## **Membership**

The core membership is set out below; representation may also be required from the Walsall Intelligence Network and other services as agreed by the Forum.

### **Coldicott Guardian**

Suzanne Joyner

### **SIRO**

Carol Williams

### **Information Champions**

Paul Gordon (Resources)

Michael Tichford (Regeneration)

Sue Butcher (Children and Young People)

Suzanne Joyner (Social Care and Inclusion)

Chris Holliday (Neighbourhoods)

David Pitches (Public Health)

### **Information Governance**

Nailah Ukaidi

Colin Teasdale

Mike Powell

### **Legal Services**

Iqbal Javed

### **Risk Management**

Pam Cox

### **Internal Audit**

Rebecca Neill





## Appendix 4 – Glossary of Terms

**Personal Data / Information:** Information relating to / about an identifiable living individual as defined under the Data Protection Act. The use of the term in this Policy is extended to include information relating to / about an identifiable deceased individual so as to address the requirements of the common law duty of confidentiality.

**Information Asset:** Information not easily replaceable without cost, skill, time, resources or a combination of these that helps to support delivery of business outcomes. Information Assets come in many forms related to information systems or business processes. E.g. databases, files, paper records, systems software, removable media, people, skills and experience.

**Safe Haven:** an agreed set of arrangements that are in place in an to ensure confidential person identifiable information (e.g. customer and staff information) can be communicated safely and securely. Safe Haven Procedures act as a safeguard for confidential information which enter or leave the organisation, whether this is by facsimile (fax), e-mail, post or other means.

**Data Subject:** an individual who is the subject of personal data. The data subject is the individual whom particular personal data is about. The Act does not count as a data subject an individual who has died or who cannot be identified or distinguished from others.

**Subject access request:** A request from or on behalf of a data subject to see information that relates to them as an individual

**Privacy Notice:** A privacy notice is the oral or written statement that individuals are given when information is collected about them. As a minimum, a privacy notice should tell people who you are, what you are going to do with their information and who it will be shared with

**Privacy Impact Assessment:** a process which helps assess privacy risks to individuals in the collection, use and disclosure of information. PIAs help identify privacy risks, foresee problems and bring forward solutions.

**Qualified Person:**

**Classification scheme** is another name for the corporate file plan, which is the shared file structure on our servers (the G: drive). The Classification Scheme used by Walsall Council is the Local Government Classification Scheme (LGCS) and it determines how records are organised.

**Metadata** describes data. It provides information about a record's content. For example a text document's metadata may contain information about who the author is, when the document was written, and a short summary of the document. Walsall Council uses the e-Government Metadata Standard (e-GMS) which defines how UK public sector bodies should label content such as web pages and documents in order to make such



information more easily managed, found and shared.

**Protective markings** are applied to sensitive information so that those handling and receiving it are aware that controls are to be implemented in order to protect it. A protective marking must be clearly visible whenever the data is viewed (in either electronic form or as hard copy). Media such as disks and tapes that contain classified data must show the protective marking on both the medium itself and its cover. Access to sensitive information or assets must only be granted to those who have a business need and the appropriate personnel security control. Casual access to protectively marked assets is never acceptable. If there is any doubt about giving access to sensitive assets, individuals should consult their managers or the Information Governance Manager before doing so.

A **record** can be defined as recorded information irrespective of medium or format (including, but not restricted to paper, microform, electronic, audio-visual) which is created, received or maintained by the council or employee of the council in pursuance of its legal obligations or in the transaction of its business. Records are a means of providing evidence of activities which support the business and operating decisions of the Council.

**e-GMS** is the UK e-Government Metadata Standard and defines how UK public sector bodies should label content in order to make information more easily managed, found and shared.

DRAFT