Cabinet – 21 April 2018

Information Governance Policy Framework (Update)

Portfolio: Councillor Keith Chambers

Related portfolios:

Service: ICT

Wards: All

Key decision: No

Forward plan: Yes

1. Summary

1.1 The Information Governance Policy Framework was developed in 2015/16 and approved by Cabinet in 2016. The over arching Framework policy is made up of three related policies:

- Records Management
- Information Security
- Information Rights

1.2 As the council prepares for the changes in Data Protection legislation through the introduction of the General Data Protection Regulations 2016, it is appropriate that the Information Governance Policy Framework is reviewed and updated. This was also a requirement noted in the 2016 ICO audit and by undertaking and approving these changes the Council is complying with these requirements.

2. Recommendations

2.1 That Cabinet approve the amended Information Governance Policy Framework and the three supporting Policies.

3. Report detail

3.1 Overarching Policy Framework

Changes within the overarching Policy Framework relate to the replacement of key definitions of legislative identifiers and or names such as Data Protection Act 1998, where these have now been updated to read General Data Protection Regulations 2016 (GDPR) and or Data Protection Act 2018 (DPA).

This also includes any requirements for updates to relationships, reporting or notification requirements and or other legislative definitions such as names,

schedules, articles and or recitals or derogations that the Council are required to apply and update.

3.2 Records Management

No key changes recorded at this point in time due to delays in national guidance or updates regarding the retention of records based on category and data type. Updates will be made to the Records management Policy contained within the Framework in line with any updated guides or codes of Practice as these occur and are proven to impact on the Councils Records Management procedures.

3.3 Information Security

The policy includes a few minor changes that align information security to Privacy by Design and will require further comment and or amendment based on the application of appropriate security standards during this process.

The final update of this policy will also require the inclusion of social media and networking requirements alongside how assurance will be gained with regards to the appropriate levels of information security regarding the diverse data types currently stored, created and or shared via the Council network.

3.4 Information Rights

This section is updated to include the General Data Protection Regulations rights of the individuals as stated by the regulations and reformed Data Protection Act 2018.

4. Council Corporate Plan priorities

The Information Governance Framework Policy supports the council's strategic priorities as set out in the Corporate Plan 2018-2020.

The use of data and information in the work of the council ensures that services are appropriate and tailored to the needs of our residents and businesses.

The key Priority which this Framework Policy supports relates to the Internal Focus in that it enables all council services to be efficient and effective. Ensuring the Council complies with the Data Protection requirements assists in improvements in service delivery through the appropriate use of accurate, up to date and available information at all times.

Data and Information is used by all services within the council, therefore the other strategic priorities fundamentally rely on quality information for decision making.

5. Risk management

The framework has been updated to include a process for the identification of data changes, ensuring there are clear processes in place for the compliance of privacy and data protection impact assessments. This will ensure that the identification of any information security or data processing risks are managed and recorded accordingly.

To further improve the ability to identify and manage risks as part of Privacy by Design, the incident management systems and reporting processes are also currently under review and will be refined and updated accordingly, potentially requiring further updates of this framework during the process.

6. Financial implications

All and any financial requirements will be captured as business as usual and do not affect the update of this framework. There is however a need for considerations to be made with regards to liability insurance as the current maximum penalty for a serious breach rises from £500.000 to £17 Million (20 Million Euros).

7. Legal implications

Failure to ensure Council Policies and procedures reflect the requirements under the reformed Data Protection Act 2018 and General Data Protection Regulations 2016 can expose the Council to significant risk of enforcement notices, monetary penalties, media exposure and or loss of services alongside criminal proceedings.

The General Data Protection Regulations increase the current maximum penalty from £500,000 to £17,000,000, therefore it is vital the Council ensures it has accurate and up to date policies and procedures in place to guide, advice and support staff and members on data processing and or sharing activities in compliance of the law.

8. Procurement Implications/Social Value (if applicable/remove if not)

Procurement implications relate to the requirements to ensure that all contracts contain the required clauses for Data Protection and the rights of individuals which are defined the Information Commissioners Office (ICO) guidance and code of practice for contractual requirements.

This relates directly to the requirements to ensure that all contracts, sharing and or processing agreements contain the required of level of control relating to the

appropriate and lawful processing conditions applied to each data processing activity.

9. Property implications

None

10. Health and wellbeing implications

None

11. Staffing implications

The Council must ensure that all staff including agency, consultants, councillors, temporary members of staff have undertaken appropriate levels of mandatory information governance, data and information security training and or refresher training on an annual basis between April 1st and March 31st of each financial year.

This is a national, legal and contractual requirement aligned to the completion of the NHS Digital Data Security and Protection (DSP) Toolkit as mandated by the Home Office, Department of Health and National Information Board. The requirements published by the National Information Board reinforce the need to build and sustain the trust and confidence of the public in the collection, storage and use of their sensitive personal data.

The framework requires that the DSP Toolkit is further developed to reflect enhanced information governance and data security requirements. Toolkit assessments must be completed and published by all bodies that process the personal confidential data of citizens who access health and adult social care services and or process or require access to NHS numbers.

12. Reducing inequalities

None affected from the original framework, however will engage with equalities to ensure the consultation is fully supported.

13. Consultation

Consultation took place by informing the Information Champions of the requirement to update the framework which was then highlighted at the monthly FIGA and addressed at the Bi weekly GDPR Project Board.

- Information Champions update Feb 7th 2018
- Forum for Information Governance Feb 22nd 2018 – notice of intention to update.
- GDPR Project Board informed 5th March 2018
- Project Sponsor and SIRO Review 22nd March 2018

14. **Communications**

The GDPR Project Team communicated the need to update this framework with Information Champions, FIGR and the GDPR Project Board throughout the project during February and March of 2018. This was recognised during the ICO audit of 2016 and work began in 2017 to draft an updated version.

Background papers
Links to relevant resources

- The General Data Protection Regulations 2016
- The Data Protection Bill 2017
- Information Commissioners Office Guidance

Author

Paul Withers
Data Protection Manager
☎ 650970
✉ Paul.withers@walsall.gov.uk

Carol Williams
Head of ICT
☎ 654881
✉ carol.williams@walsall.gov.uk

Tony Cox
Head of Legal and GDPR Project Sponsor
654822
Anthony.cox@walsall.gov.uk

James Walsh
Executive Director

17 April 2018

Councillor Chambers
Portfolio holder

17 April 2018

Information Governance Policy Framework

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

Authors: Paul Withers
Caroline Hobbs
James Sparrock
Version: V 2.5
Status: DRAFT
Version Date: March 2018
Revision Date: May 2020

Contents

1.0 Policy Statement 6
2.0 Purpose 8
3.0 What is Information Governance? 9
4.0 Applying the Policy Framework 10
5.0 Delivery 10
6.0 Information Governance Roles and Responsibilities 13
7.0 Strategic Implementation 15
8.0 Governance and Compliance 15
8.1 Employees 15
8.2 Elected Members 15
8.3 Others Working on Behalf of the Council 16
8.4 Responsibilities 16
Part 1: Information Risk and Security Policy 17
1.1 Policy Statement 17
1.2 Scope 18
1.3 The Policy 19
1.3.1 Information Assets & Risk Management 19
1.3.2 Information Asset Security & Confidentiality 19
1.3.3 Access Controls 20
1.3.4 Equipment Security 21
1.3.5 Mobile Working 21
1.3.6 Timeout Procedures 22
1.3.7 Use of Removable Media 22
1.3.8 Information Classification 22
1.3.9 Posting, emailing, faxing and printing information 22
1.3.10 Physical and Environmental Security 24
1.3.11 Equipment and Data Disposal 24

1.3.12 Intellectual Property Rights 24

1.3.13 Systems development, planning and procurement 24

1.3.14 Data Changes 25

1.3.15 Cyber Security 26

1.3.16 Cloud Storage Services 27

1.3.17 Information Sharing 28

1.3.18 Breach Management 28

1.3.19 Business Continuity Planning 28

1.3.20 Contracts 28

1.3.21 Contracts of Employment 28

1.3.22 Personal Use 29

1.3.23 Public Groups using ICT Services provided by the Council 29

1.3.24 Social Networking and Media Platforms 29

Part 2: Information Rights Policy 32

2.1 Policy Statement 32

2.2 Scope 32

2.3 The Policy 32

2.3.1 Freedom of Information (FOI)/Environmental Information Regulations (EIR) 32

Making a request 32

2.3.1.2 Environmental Information Regulations 33

2.3.1.3 Advice and Assistance 34

2.3.1.4 Handling Requests 34

2.3.1.5 Timing of Requests 34

2.3.1.6 Refusing a Request 34

2.3.1.7 Qualified Person 35

2.3.1.8 Consultation with Third Parties 35

2.3.1.9 Contracts 35

2.3.1.10 Repeat Requests 35

2.3.1.11 Publication Scheme 35
2.3.2 Subject Access Requests 35
2.3.2.1 Confirming Identity 36
2.3.2.2 Handling Requests 36
2.3.2.3 Timing of Requests 36
2.3.2.4 Access to Personal Data by an Authorised/Legal Agent 36
2.3.2.5 Access to Personal Data of a Child 36
2.3.2.6 The Mental Capacity Act 37
2.3.2.7 Information Containing Third Party Data 37
2.3.2.8 Access to Records of Deceased Individuals 37
2.3.2.9 Refusing a Request 37
2.3.3 Privacy Notices 37
2.3.4 Amendments to Inaccurate Records 37
2.3.5 Objections to Processing 38
2.3.5.1 Direct Marketing 38
2.3.5.2 Prevention of Processing Likely to Cause Substantial Damage or Distress 38
2.3.6 Releasing personal information to prevent or detect crime 38
2.3.7 Complaints 39
Part 3: Records Management Policy 40
3.1 Policy Statement 40
3.2 Scope 41
3.3 The Policy 41
3.3.1 Legislation 41
3.3.2 Records Creation 41
3.3.3 Records Classification 41
3.3.4 Metadata 41
3.3.5 Protective Marking 42
3.3.6 File naming 42
3.3.7 Record Storage, Security and Maintenance 42

3.3.7.1 Storage of Physical Records 42
3.3.7.2 Storage of Electronic Records 43
3.3.8 Version Control 43
3.3.9 Retention and Disposal of Records 44
3.3.10 Data Quality Assurance 44
3.3.11 Historical Records 45
Appendix 1 – Legal Requirements, Regulations and Standards 47
Appendix 2 - Related Council Procedures and Guidance 49
Appendix 3 – Forum for Information Governance and Assurance 50
Appendix 4 - IG User Account Access Request Form 54

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 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 Framework also establishes a culture of individual responsibility for information governance, informed and supported by awareness and training for employees, elected members and others working for or 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 employees, elected members and anyone else working for or on behalf of the council i.e. partners, contractors and agents.
Non compliance with this Framework and the associated Polices 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 and contractual 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 while complying with the Data Protection Regulations and Information Security 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, 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 employee compliance with the Information Governance Policy Framework through regular audits and reports.

The Information Governance Policy Framework is addressed in three parts:

1. **Part 1: Information Risk & Security Policy** – including:
    - Confidentiality and Data Protection
    - Information sharing and processing
    - Data privacy and information security impact assessments
    - Information and cyber security
    - Social media and networking controls

2. **Part 2: Information Rights Policy** – including:
    - Freedom of Information
    - Environmental Information Regulations
    - Privacy and Electronic Communications Regulations
    - The Data Subjects rights, under the General Data Protection Regulations 2016 (GDPR) and the UK Data Protection Act 2018 (DPA).

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 the 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.

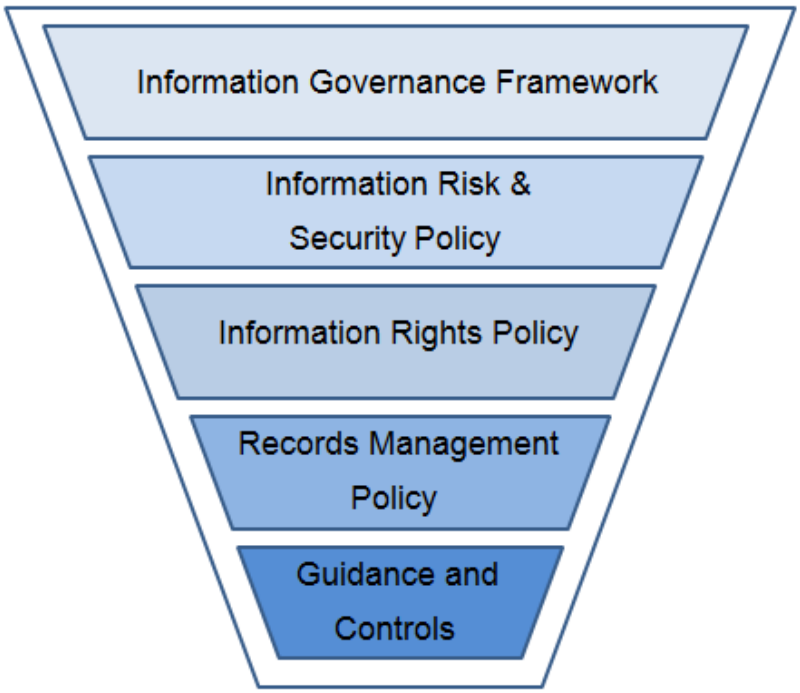


Fig 1: Information Governance Framework

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

2.0 Purpose

The Information Governance Policy Framework 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 within the council takes many forms including data stored on computers, transmitted across networks, presented on web pages, printed or written on paper, sent by fax, stored on tapes, CDs, DVDs or spoken verbally, directly or indirectly.

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:

- Affective identification, management and or mitigation of information, risks, breaches and incidents.
- Appropriate and adequate processes and awareness to support the duty of confidentiality and compliance of the data protection regulations.
- Improvements in information handling and processing activities.
- Increased customer confidence in the council and its staff with regards to information collection and processing.
- Supported sharing of lessons learnt and best practice.

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 by the council are sourced, held and used appropriately, securely and legally.
Information governance ensures appropriate controls, responsibilities and actions for the security, confidentiality and protection of information is embedded into the Councils business as usual and covers all information held by the council (for example – employee, financial, estates, corporate) and all "information systems" (assets) used to hold that information.

Systems may be purely paper-based or partially or totally electronic. The information concerned may be "owned by" or required for use by the council and hence may be internal or external.

As a provider of a wide range of services, the council carries a responsibility for handling and protecting information of many types and categories. These types of information include personal data, commercially sensitive/confidential data and non–confidential/public data alongside business critical information.

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 the council's commitment to transparency and the Open Data agenda alongside the requirements for Privacy by Design (PbD).

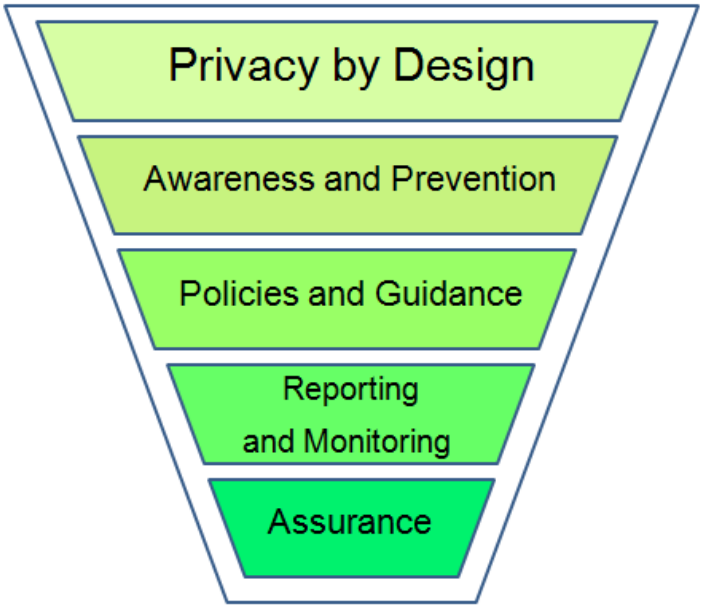


Fig 2: Privacy by Design Framework

Good Information governance will enable the council to meet national, legal requirements including annual submissions of Public Services Network (PSN) compliance and the Data Security and Protection Toolkit (a performance tool, updated by NHS Digital in 2018

with the purpose of measuring an organisations compliance with national information governance standards and relevant legislation which permits access to the NHS and public sector networks).

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 must comply.

4.0 Applying the Policy Framework

In adopting this Information Governance Policy Framework, 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.

5.0 Delivery

Through implementing this Framework, the council will:

- establish robust information governance processes conforming to statutory requirements and national standards
- ensure that all practices and procedures relating to collection, processing and or sharing of personal, sensitive and council corporate information are legal and conform to best and/or recommended practices or standards
- 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 appropriate levels of security are applied at all times, e.g. through the use of data protection impact assessments (DPIA – formerly known as PIA) and or information security 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 and maintenance of council information assets
- maintain a clear reporting structure and ensure through management action and training that all individuals working for or on behalf of the council understand information governance requirements alongside the duties of confidentiality and data protection.
- undertake reviews and audits of how information is recorded, held and used. Management audits will be used to identify good practice and opportunities for

improvement alongside the mitigation of identifiable risks.

- 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 information governance breaches and security incidents in line with the council's Information Risk and Security Policy, which forms part of this Framework
- assess its own performance using the Data Security and Protection Toolkit and PSN compliance requirements and maintain, develop and implement action plans to support continued improvement for the assurance of legislative and or contractual compliance.
- ensure all employees undertake the appropriate level of Information Governance Awareness training for their role on an annual basis. The requirement of any further information risk and security or records management training will be subject to the role of the individual 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 and transparency

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 as Information Asset Owners (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.
- Ensure that appropriate reports and records are maintained in line with the requirements to capture and assess processing activities.

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 relevant law and regulation including the GDPR and UK Data Protection Act, the Human Rights Act, the Common Law Duty of Confidentiality and all associated guidance
- establish and maintain policies or procedures for the controlled and appropriate sharing of information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act) or any other requirements for data sharing in accordance with national contracts and or public tasks.

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 GDPR/UK Data Protection Principles.
- Identify and classify information to ensure that is handled and shared appropriately.
- Ensure effective reports, processes and records are in place to provide information asset owners with the ability to identify risks and take actions.

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

- Ensure the Council embeds and monitors data protection by design by proactively assessing changes to way we create, use, store and or share information.
- Ensure systems are in place to recognise information assets and owners.
- Ensure systems and or processes are in place to recognise, identify and take action against information risks.
- 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.
- Ensure appropriate Privacy Notices are in place to capture the requirements of GDPR in providing data subjects with adequate and appropriate information over the way in which the council collects processes and shares information while ensuring the rights of individuals are clearly identified.

6.0 Information Governance 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 also attended by the Data Protection Manager and Information Security Officer alongside any other representation as required to ensure compliance of the regulations is upheld.

FIGA is responsible for ensuring that any risks identified are addressed and for providing 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. The Terms of Reference and membership are attached at Appendix 3.

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. To coordinate data protection and privacy by design. This function will also act in an advisory capacity to the 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 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	Champion awareness, understanding and compliance with the key principles of information governance. Members of FIGA. Responsible for ensuring key messages and actions are disseminated appropriately throughout the directorates.
Information Asset Owners	Designated senior officers with ownership and responsibility for specific information assets (paper based and electronic records and IT systems). IAO's must identify and document the availability requirements for their systems and formulate a contingency plan in the event of system failure. Supported by Information Asset Custodians.
Information Asset Custodians	Designated officer with responsibility for day to day management and protection of specified information assets. (paper-based records and IT systems).

7.0 Strategic Implementation

FIGA will monitor implementation of this Policy Framework through regular meetings which will involve:

- ensuring the development and review of policies and procedures required for information governance and having final approval of these documents.
- Ensuring appropriate resources are in place to achieve compliance of the regulatory requirements.
- Reporting on progress, incidents and issues to CMT/elected members.

This Framework will be reviewed bi-annually or as required in response to any significant legislative changes, mandatory requirements, national guidance or as a result of significant information governance breaches or incidents and approved by FIGA, CMT and the councils full Cabinet.

Information Asset Owners will be a key part of this process as they are the officers accountable for information assets across the council and are responsible for ensuring that appropriate information governance arrangements are in place locally and that national or legal requirements are met.

8.0 Governance and Compliance

Non-compliance with this Framework and relevant policies could potentially expose the council and/or its customers to risk. The potential impact of damage or loss of information includes disruption to services, risk to citizens, damage to reputation, legal action, personal distress, loss of confidence, or media coverage and may take considerable time and cost to recover.

8.1 Employees

All new employees (including school–based staff) will receive awareness training and guidance on information governance, which will include:

- Confidentiality
- Data Protection
- Information and Cyber Security
- Information Rights

All employees will be required to repeat their information governance awareness training annually between April and March.

Employees who do not comply with these policies/procedures may therefore be subject to disciplinary action, in line with the council's disciplinary procedures.

8.2 Elected Members

All elected members will also receive annual awareness training and guidance on information governance, which will include confidentiality, data protection, information security and cyber security alongside lessons learnt and proactive data security notices. Members' failure to comply with these policies/procedures will constitute a potential breach of the council's Member's Code of Conduct and associated Member/Officer Protocol.

8.3 Others Working on Behalf of the Council

Any persons working for and on behalf of the Council must undertake appropriate awareness training prior to gaining access to Council held information or business critical data/systems. All managers are therefore responsible for ensuring that any person, agent, consultant, temporary or honorary member of staff must comply with national, legal and local information governance awareness and abide by the duties of confidentiality and data protection.

8.4 Responsibilities

The Data Protection Manager shall have overall responsibility for managing and implementing the Framework and related policies 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 this Framework and the policies 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
- Received appropriate and up-to-date training relating to information governance.
- Abide by the Councils Code of Conduct

Non-compliance with these policies/procedures may therefore be subject to disciplinary action, in line with the council's disciplinary procedures and or legal action if appropriate.

The following table identifies who within Walsall Council is Accountable, Responsible, Informed or Consulted with regards to this Framework. The following definitions apply:

- **Accountable** – the person who has ultimate accountability and authority for the Framework.
- **Responsible** – the person(s) responsible for developing and implementing and reviewing the Framework.
- **Consulted** – the person(s) or groups to be consulted when the Framework 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

Part 1: Information Risk and Security Policy

1.1 Policy Statement

Information is a vital asset to the organisation. Walsall 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 appropriate use of information in supporting customer demand and normal business activity for the council and other organisations that it works with. Information must be accompanied by appropriate levels of security at all times. 'Appropriate' is a degree of precaution and security proportionate to the potential risk, information category and impact of loss or accidental disclosure.

The Information Risk and Security Policy will ensure an appropriate level of:

Confidentiality

To ensure the confidentiality of information is achieved, access to Information is controlled and monitored accordingly based on the data category requirements, roles of individuals and processing conditions. Information is only accessible by those who require it and only disclosed lawfully where appropriate controls and assessments have been undertaken. Systems and information assets must also ensure that appropriate levels of security are in place at all times to protect the confidentiality of the data held within.

Integrity

Information must be accurate and up to date in accordance with the Data Protection Act and Regulations under GDPR alongside the rights of the individuals with regards to rectification and erasure. All information assets and systems must be assessed regularly to ensure compliance of these requirements.

Availability

Networks, systems and information assets should always be available when required to those with a justified right to access. This relates to

business continuity and systems resilience which ensure that data remains available and secured

Anyone handling personal, sensitive or confidential information must take personal responsibility and make considered judgments in terms of how it is handled whilst delivering council services. If in any doubt members of staff and or systems users should always seek advice from the Information Security Officer or Data Protection Manager.

The Information Risk and Security Policy will also make sure that:

- the council establishes a culture of care and security for information.
- information is only obtained or shared when it is required
- information owned or processed by the council is protected against unauthorised access or disclosure
- ICT equipment is protected from accidental or malicious damage
- information security risks are properly identified, assessed, recorded and managed
- Information security incidents are reported and managed appropriately.
- appropriate safeguards are implemented to reduce security risks
- legal and regulatory requirements are understood and met
- guidance and training with regards to information security is available and up- to-date.

Compliance with this policy will be achieved by:

- ensuring that all individuals who work for or on behalf of the council are aware of and fully comply with the relevant legislation as described in this and other policies and procedures

o Introducing a clear process for the recognition of data changes and the appropriate application and completing of data privacy impact and information security risk assessments.

o Ensuring that any assessments identify appropriate measures for risk identification and reduction.

- introducing a consistent approach to security, ensuring that all individuals who work for or on behalf of the council fully understand their own responsibilities and have the appropriate tools to work with
- creating and maintaining a level of awareness of the need for information security as an integral part of day to day business
- reporting and investigating all breaches of information security, actual or suspected.

1.2 Scope

This policy applies to all individuals working for or on behalf of the council who use or have access to council information assets, computer equipment or other ICT facilities.

The policy applies throughout the lifecycle of the information from creation though storage, use and transfer to retention and disposal. It applies to all information including, but not limited to:

- information stored electronically on databases or applications both on site or in the Cloud
- information stored on computers, PDAs, mobile phones, printers, or removable media such as hard disks, CD, memory sticks, tapes and other similar media
- information transmitted on networks or via the internet and or social media platforms
- information sent by email, fax or other communications method
- all paper records including information sent out by post
- 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

All council information assets must be risk assessed and measures put in place to ensure each asset/system is secured to an appropriate level based on the measure of risk associated with it. This process will involve identifying threats and vulnerabilities (severity of impact and the likelihood of occurrence) at an individual asset level and the analysis and assessment of risks in order to make the best use of resources.

Information security risks must be recorded within a baseline risk register and action plans put in place to effectively manage those risks. The risk register and all associated actions must 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.

Overall responsibility for information security risk management will rest with the SIRO but day to day management will rest with the IAO's and Information Custodians with support from the Information Security Officer where required.

1.3.2 Information Asset Security & Confidentiality

Information risk and security management controls and procedures for all information assets will conform to the International Standard for Information Security ISO27001:2013 and the associated code of practice ISO27002:2013.

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 council's ICT systems, processes and infrastructure will be designed and maintained to ensure that:

- Appropriate measures are in place to protect the council's information and systems from damage or loss due to malicious software such as viruses and or cyber attacks.
- Information is available when required i.e. by ensuring that information and information systems are available to authorised users at point of need and

appropriate business continuity and disaster recovery processes are in place and audited regularly for functionality.
- Robust password and access control regimes are in place and maintained.
- Managers are aware of their responsibilities with regards to authorizing and monitoring systems access.
-

Where equipment and devices are no longer required the ICT service will ensure that devices are appropriately cleansed for reissue or destroyed in accordance with the internal processes requirements and national standards.

Equipment will not be reallocated or reissued without appropriate data cleansing in line with the government standards such as IS5 (information security standard).

External or third party systems: In addition to the above, line managers must also ensure that they follow any password and or security controls applied by third parties and that appropriate agreements or controls are in place to ensure secure access to information being shared with the council and utilized within the network.

1.3.3 Access Controls

Individuals given access to council information assets should only access systems that they have authority for. Under the Computer Misuse Act (1990) it is a criminal offence to attempt to gain access to computer information and systems without authority to do so. Unauthorised access to information systems or information contained within a system will also be recognized as serious breach of confidentiality under the data protection regulations.

Systems access:
Formal procedures are used to control access to IT systems. Most systems employ role based access controls (RBAC) where access is granted based on a users role and justified requirements.

Least privilege basis access (users are only granted access to parts of the network, systems or applications that their job role requires). In some cases this may result in view only access being granted unless otherwise justified and authorised.

For access to be granted, an authorised manager must contact ICT by email or using the work request process stating the access level required.

Leaving or moving:
When individuals leave the organisation or move to another team/service it is their manager's responsibility to ensure that access is amended or accounts are disabled/deactivated. User access rights will be reviewed, monitored and audited on a regular basis (at least annually).

Account access:
User activity can also be monitored where an information security breach or incident requires further investigation.

Where there is a justified requirement to access information contained in a member of staffs email account, home drive or shared area, the senior manager must complete the IG Account Access Request Form. The form will be used to verify the requirement and ensure appropriate access is granted on a need to

know basis. The form should then be returned to the information governance and assurance team for approval or further information/actions.(see appendix 4)

Once a form has been completed the following process will be completed:

- The formal review of the access request and permissions required
- Approval or denial of the request in accordance with justification and rights of the individuals concerned
- Password access request sent to ICT
- Formal review arranged with appropriate senior lead
- HR Representative informed of actions if required.
- Senior lead or manager and Information Governance and Assurance Officer Review information required and gain access.
- Account reset so that user requires new password on return
- Where justified user provided with notice of access

In the event that access is required in line with disciplinary actions, breaches of data protection or criminal investigations the Information Governance and Assurance Team will include a HR representative.

Password Management:
Passwords must be changed when prompted and strong passwords should be used e.g. 15 characters including at least one capital letter one lower case letter and a special character (!£$%&*). Passwords must not be written down or shared with anyone else. A short memorable phrase can be used to aid memory.

Third Party Systems Access:
Third parties requiring access to council systems for maintenance and support must sign a 3rd party access agreement before access is granted or be supervised on site by a member of ICT staff.

1.3.4 Equipment Security

To mitigate the risks of loss, damage, theft or compromise of equipment and to protect equipment from environmental threats and hazards, and opportunities for unauthorised access:

- equipment in the council's data centre will be protected from disruptions caused by failures in supporting services e.g. power failure, air conditioning failure
- all equipment will be correctly maintained to ensure correct (specified) operation and uptime
- security settings and software must not be altered without prior permission from ICT.
- Regular patches and software updates are applied in line with the ICT patch process. These ensure the council is operating its network and systems using the latest safeguards and security controls.

1.3.5 Mobile Working

Mobile working is permitted and is subject to prior approval and the following precautions must be adhered to:

- always ensure devices or information are protected appropriately in accordance with this Policy and Framework.

- always work in an appropriate environment that ensures the confidentiality and security of any information being accessed.
- never install or use unapproved software or memory devices.
- never leave mobile devices in open areas, unattended vehicles or unsecure locations.
- never provide access to unauthorised or unapproved persons.
- never remove the security or access controls applied to council devices
- never store passwords with devices.
- ensure devices are charged regularly and logged on and connected to the council network at least once a month for a period of at least two hours so that appropriate patches and security updates can be applied.
- report any loss or theft of mobile devices immediately to your direct manager and the ICT Service Desk - 01922 652862.

1.3.6 Timeout Procedures

Inactive computers are set to time out after a pre-set period of inactivity. The time-out facility will clear and lock the screen.

Users must lock their computers, if leaving them unattended using the Ctrl/Alt/Delete or Windows and L keys. (see image below)

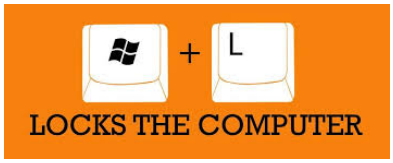


Fig 3: Quick lock Option

1.3.7 Use of Removable Media

It is the council's policy to prohibit the use of all unauthorised removable media devices including USB sticks. The use of removable media devices will only be approved if a valid business case for its use is provided.

The council issues approved encrypted USB memory sticks for the transfer of council data (including Sensitive and Person Identifiable Data). The process for obtaining a USB stick and the associated Procedure for the Use of Removable Media can be found on the Information Governance Intranet pages on the inside walsall.

1.3.8 Information Classification

All information within the council will be identified and classified by the criteria set out in the council's Protective Marking Procedure which is available on the Information Governance pages on the intranet.

This will ensure that information is given the appropriate level of protection when it is processed. Classification may change at any point in the information lifecycle e.g. a document may have a different classification when it is created to when it is approved and available for circulation. Information that is not classified will assume the lowest classification of 'Not Protectively Marked'.

1.3.9 Posting, emailing, faxing and printing information

When sending information either inside or outside the council the appropriate

method of transmission must be used according to the confidentiality or sensitivity of the information and the classification it has been given.
The risk of harm or distress that could be caused to the individual(s) that the information relates to if it were lost or sent to the wrong recipient should be considered when making the decision on the most appropriate method of transmission. Contact the Information Security Officer for guidance if required.

It is important that only the minimum amount of information required is sent, by whichever method is chosen.

When sending information by email the sender must:

- carefully check the recipient's email address before pressing send – this is particularly important where the recipient fields are automatically populated by the system
- take care when using the 'reply to all function – are all the recipients known and do they all need to receive the information being sent
- ensure that personal, sensitive or confidential information is not included in the subject field or body of an email. If sensitive information has to be sent via unsecure email, password protected attachments must be used. A different transfer method must also be used to communicate the password e.g. telephone call, separate email or text
- secure email must always be used for sending personal, sensitive or confidential information if it is available
- the use of personal or home email addresses for council business is strictly prohibited.
- when using email to communicate with other public sector network partners such as health, police or local authorities always use the approved secure email system (e.g. gcsx, gsi, cjsm etc), especially when sharing personal, confidential, sensitive information. Further information can be found on the intranet under - Methods of transferring personal information securely

When sending information by post the sender must:

- ensure that the name and address details are correct – window envelopes should be used whenever possible to avoid errors in transcribing details
- ensure that only the relevant information is in the envelope i.e. the information is adequate, relevant and not excessive.
- that envelopes containing personal, sensitive or confidential information are marked 'private and confidential – addressee only'
- that a return address is added/printed on the back of the envelope

When sending information by fax the sender must:

- telephone ahead to advise the fax is being sent and ask for confirmation of receipt
- check the fax number is correct and dial carefully
- attach a cover sheet to the fax indicating who it is for, the fax number it has been sent to, the contact details of the sender, the date and number of pages (including the cover sheet) in the document
- if the information is particularly sensitive (and it cannot be sent by a more secure method) consider sending a test fax to ensure it reaches the correct recipient

When printing or photocopying information always ensure that:

- secure printers are used wherever possible

- if unsecure printers are to be used, only ever print the minimum required.
- prints are always collected immediately
- check the document to ensure you have collected every print out
- ensure the printer has enough paper to complete your print
- where you require large print runs always consult the Print and Design service
- ensure multiple documents are separated accordingly to avoid misfiling

1.3.10 Physical and Environmental Security

Depending upon the function and the nature of use, offices where information is held will be equipped with appropriate security controls e.g. CCTV, entry controls etc. Public areas, deliveries etc. will be isolated from information processing areas.

Offices that deal with personal and/or sensitive information will have entry controls and lockable storage facilities.

ID cards, keys and other entry devices must be returned when access is no longer required.

All visitors must have official identification passes issued by the council. If temporary access to systems is given a 3rd party access agreement must be signed and access must be disabled when the visitor leaves. Visitors should not be afforded opportunity to view computer screens or printed documents without authorisation.

Physical security to central building is controlled by the COTAG access control system. Strangers in office areas without an ID badge should be challenged or reported. Tailgating is not permitted.

Anyone handling personal, sensitive or confidential information is required to clear paperwork from their working area when leaving it for any length of time and always at the end of each working day Paperwork should be locked away securely.

1.3.11 Equipment and Data Disposal

If a device has ever been used to process council data, action must be taken to ensure data is irrevocably removed as part of the disposal process. All equipment that is past its useful life must be returned to ICT for disposal. The council has a documented procedure for the disposal of equipment.

1.3.12 Intellectual Property Rights

All users must ensure that only licensed software issued or approved by ICT is installed on council equipment. The loading and use of unlicensed software on council computing equipment is not permitted. All users must comply with the Copyright, Designs and Patents Act (1988). This states that it is illegal to copy and use software without the copyright owner's consent or the appropriate license to prove the software was legally acquired. The council monitors the installation and use of software. Any breaches of software copyright may result in personal litigation by the software author or distributor and may be the basis for disciplinary action under the council's disciplinary procedures.

1.3.13 Systems development, planning and procurement

All system developments must comply with the council's ICT Strategy. Security and risk management issues must be considered and documented during the

requirements and procurement phases of all procurements and developments which affect data relating to council activity, council customers, partners, employees or suppliers.

Privacy by design is an approach that promotes privacy and data protection compliance from the start. The General Data Protection Regulations (GDPR) has introduced a legal requirement for Data Protection Impact Assessments and privacy by design in certain circumstances.

The council will, therefore, ensure that privacy and data protection is a key consideration in the early stages of any project, and then throughout the project lifecycle. Projects would include (but not limited to):

- A new IT system
- A new data sharing initiative
- A proposal to identify people in a particular group or demographic
- Using existing data for a new or more intrusive purpose
- Introduction of a new CCTV system or the application of new technology to an existing system

IT systems are checked both internally and by external accredited suppliers on a regular basis for security and technical compliance with relevant security implementation standards including:

- Public Services Network connection
- Payment Card Industry Data Security Standard (PCI/DSS)

1.3.14 Data Changes

In order to gain assurance that information is handled securely, legally and in line with any legislation or IG requirements the inclusion of Information Governance and Privacy must be taken into account at the beginning of new projects or processes that affect the way in which information is handled.

Services must not purchase new systems, mobile technology devices, and external services or implement process changes that involve the use, creation, storage and or sharing of personal, sensitive or confidential data without first completing the IG Data Change Request Form.

This form will help the Information Governance and Assurance Team determine which IG assessment process your new project or change in data handling will require.

We will also pass your completed form onto the Information Security Officer to ensure the ICT Change process is adhered to in line with section 1.3.13.

Depending on the information you provide we may ask you to complete:

- Information Security Assessment (ISA)
- Data Protection Impact Assessment (DPIA)

- Site or Premises Assessment form

Where data processing is involved it may also be necessary to ensure that IG or DPA (Data Protection Act) clauses are included in contracts and or sharing, processing agreements.

The Information Security Officer and Information Governance and Assurance Team undertake assessments to provide assurance that all personal/confidential information is secure in accordance with the GDPR, DPA and DSP Toolkit requirements.

If data is to be held on third party premises the Information Security Officer may also need to undertake a Premises or Technical Security Assessment.

Next Steps:
Please make sure you consider the following points before ordering, buying or making changes to the way in which data is held or collected within the Council:

- Is this something that includes the storage or use of service user/staff information?
- Are you changing a process, contract or Service Level Agreement (SLA) that involves service user/staff information?
- Are you purchasing something that will be used for the processing of service user/staff information?
- Are you purchasing something that will be used for the processing of business information?
- Is a third party organisation going to be processing any personal or special category (sensitive) data on your behalf?
- Have you contacted the Information Security Officer to make them aware of your project?

If you have answered yes to any of the above questions, then you will need to complete the IG Data Change Request form.

If you are experiencing any difficulty or require some additional information please call the Information Governance and Assurance Team on 01922 65 0970

The required form can be found on Inside Walsall under Information Governance – Data Changes.

1.3.15 Cyber Security

Cyber security and cybercrime are persistent threats that, if left unchecked, could disrupt the day to day operations of the council, the delivery of local public services and ultimately have the potential to compromise national security. In the event of a successful attack this may also result in loss of data, potential for monetary penalties and additional replacement systems or equipment costs to rectify any data losses or disclosures and or systems functionality.

Technical advances create opportunities for greater efficiency and effectiveness. These include more engaging and efficient digital services, new ways to work remotely and to store and transfer data, such as mobile devices and cloud services.

The scale of targeted attacks, coupled with the difficulty of monitoring all possible attack methods requires the public sector to work together to both reduce the likelihood and the impact of such a threat succeeding.

Foreign states, criminals, hackers, insiders and terrorists all pose different kinds of threats. They may try to compromise public sector networks to meet various objectives that include:

- financial gain
- attracting publicity for a political cause
- embarrassing central and local government
- controlling computer infrastructure to support other nefarious activity
- disrupting or destroying computer infrastructure stealing sensitive information to gain economic, diplomatic or military advantage

Council employees can also be targets for criminal activity.

As with most local authorities, Walsall Council relies heavily on access to the internet and to information held in its systems. There are several IT systems/services that have an internet presence e.g. the council website or the ability to work from home and there are several different ways gain access to information e.g. Wi-Fi, physical networking, mobile phones, tablets etc. All can present threats to cyber security. It is widely acknowledged that it is not currently possible to keep out all attacks all of the time, but the council employs a range of tools and good practice to minimise the risk to its information and systems.

The council has clear procedures and guidance on Information Security, which provide information on a range of areas including:

- Reporting of security incidents
- Use and security of emails
- Use of the internet
- Mobile phone usage
- Removable Media
- Sharing and disclosing information

These documents can be found on the Information Governance pages on the intranet.

The council implements security controls and good practice to enable it to achieve compliance with Public Services Network (PSN), Payment Card Industry Data Security Standards (PCI DSS) and the NHS DSP Toolkit. All of these require the council to ensure that systems are security patched and that the council has regular penetration tests of its network/systems that are performed by a third party.

1.3.16 Cloud Storage Services

The use of open cloud storage solutions (Skydrive, Onedrive, iCloud Dropbox etc.) for the transfer of council information is not permitted unless express permission is granted by the appropriate IAO and the Information Security Officer. These tools must never be used to transfer personal or confidential information. For advice on the secure methods available to transfer council data contact the Information Security Officer.

Where the use of external cloud services is required, the ICT department, Information Security Officer and SIRO will ensure that appropriate assessments and controls have been undertaken and or applied, to provide the level of assurance for information security required.

1.3.17 Information Sharing

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 is subject to appropriate information sharing/processing agreements and the requirements of the GDPR and Data Protection Act. Information sharing with other external organisations should also be supported by a purpose specific information sharing/processing agreement. 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 and Assurance Team and the Information Security Officer and signed by the relevant Information Asset Owner(s) in all participating organisations/teams. Approval should also be sought from the SIRO and/or Caldicott Guardian where appropriate.

1.3.18 Breach Management

The council's Procedure for Reporting and Managing Data Breaches must be followed wherever there is any unauthorised or unlawful disclosure, loss, damage or destruction to personal or confidential information. Anyone granted access to council information is responsible for reporting any actual or suspected breach as soon as it is discovered and must be aware of the procedure and the reporting requirements.

1.3.19 Business Continuity Planning

All systems and information assets will have threats and vulnerabilities assessed by system owners to determine how critical they are to the council. Individual directorates 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. The Council's business continuity planning process will include consideration of information security gained from the information asset and risk register.

1.3.20 Contracts

If contracts involve exchange of personal or sensitive data a DPIA must be completed and approved and if services are hosted elsewhere a Technical Assessment must also be completed and approved as part of the procurement process.

Prior to award of a contract a Data Processor Agreement or Contract must be implemented and signed by any 3rd party handling personal information on behalf of the council providing assurance that they comply with the GDPR and theData Protection Act requirements if processing relate to personal or special category (sensitive) data.

All new contractual arrangements with suppliers of goods or services to the council will contain confirmation that the suppliers comply with all appropriate information security policies and procedures in accordance with the guidance on contractual clauses as provided by the Information Commissioners Office

1.3.21 Contracts of Employment

Information security expectations of employees shall be included within job descriptions and person specifications where appropriate.

Pre-employment checks will be carried out in accordance with relevant laws and regulations and proportional to access to information and business requirements this may involve requirements for BPSS/DBS checks.

Employee security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain a confidentiality clause.

Annual information governance training is a national legal requirement that the council must comply with. The council's IG training plan is managed by the Information Governance and Assurance team who will ensure all employees are aware of the training they need to undertake.

1.3.22 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 Procedure (Section 4.2) and other procedures relating to the use of council devices.

1.3.23 Public Groups using ICT Services provided by the Council

Certain groups outside the control of Walsall Council management may use the council's ICT services – e.g. libraries provide the public with internet access and certain areas are covered by WiFi provided by the council. Conditions of use and security measures in place will fall outside of this policy and will be managed separately.

1.3.24 Social Networking and Media Platforms

The Home Office states that it is very apparent that more and more government bodies are now looking to present themselves via social networking tools.

In order for the Council to improve its accessibility and visibility on social media sources, a policy and supporting guidance is required to ensure that any regulatory or professional, legal requirements are fully understood and met.

This policy provides staff with clear guidelines on:

- acceptable use of social media linked to their employment
- acceptable use of social media for the purpose of Council business
- being mindful of any content they share on such platforms
- maintaining appropriate standards of confidentiality
- maintaining and protecting professional boundaries with service users

The use of social media for and in private are not covered within this policy as all staff must follow professional codes of conduct, employment contracts and Council policies at all times.

Council employees will not use or maintain a social networking site that contains:

- Personal identifiable information of Council service users and/or their relatives
- Personal identifiable information of other Council employees in relation to their employment, including judgements of their performance and character
- Photographs of other Council employees or service users taken for the purpose of social networking without full and explicit consent in line with the consent guidance.
- Statements that bring the Council, its services, its staff or contractors into disrepute
- Council confidential or business information must not be loaded onto a private or business social networking site without the appropriate senior managerial sign off and without compliance of the Council publication scheme.
- Employees must examine carefully any email or message coming from social networking sites or contacts, as these may be unreliable, contain malicious codes, be spoofed to look authentic, or may be a phishing email
- Employees should not conduct themselves in ways that are detrimental to the organisation or service.
- Employees should take care not to allow their interaction on these websites or platforms to damage working relationships between members of staff and service users.

Any staff wishing to set up social media sites for their department or services must seek permission from the communications department and Information Governance and Assurance Team before doing so.

Information security is implemented to protect and provide adequate security levels for information containing personal, sensitive and or confidential information relating to an individual or the business. It is vital that Social Networking forms part of this policy and supports this policy in order to protect the organisation, its staff and ensure that at all times the Council are fully compliant with any Data Protection Regulations or legal requirements.

There are 3 main elements for the use of social media sites within Council services or functions:

- Permission:
  - Service leads and managers must gain IG and Communications sign off for the creation and or use of social media sites and outlets. This is undertaken via the “IG Request Form for data changes” (see appendix).
  - Unauthorised use of social media to promote the Council is a breach of these policies and will be managed in line with Council disciplinary proceedings and potential dismissal or suspension.
- Integrity
  - Ensuring that information is accurate and can be modified by authorised persons only
  - Services must follow policies for the use of a social network, site or any external web application.

- Accountability
  - Service leads and Information Asset Owners are responsible for ensuring that those using social media to support services as part of a business function, comply at all times with the required and appropriate policies, procedures and codes.

This will ensure that the Council complies with legislation and standards relating to the use of social media, including the Computer Misuse Act, ISO27001 (International Standards for Information Security) and the Confidentiality Code of Practice: Information Security Management and the NHS Digital DSP Toolkit requirements.

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:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling

Anyone can make a request for information held by the council under the Freedom of Information Act 2000 or the Environmental Information Regulations 2004. Requests for personal information can also be made by the individual the information relates to under the GDPR.

2.2 Scope

This policy relates to all services of the council and all information created and received by the 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)

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 and Assurance 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. Requests made 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 and Assurance 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 from the date the request is received by the council. The requester should be kept informed of any delays or extensions to these timescales.

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, under normal circumstances, only the 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 GDPR 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 Data Protection 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

To be a valid subject access request under the GDPR, requests:

- must be in writing and be legible
- must follow the process of confirming identification

- 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 GDPR requests **do not:**

- have to be submitted on a specific form
- need to mention the GDPR or the term 'subject access' or
- need to have been received directly by the Information Governance and Assurance 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 and Assurance Team, where a valid request is received under the GDPR, 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 a response must be provided no later than 1 month from the day of receipt, unless the case is considered to be complex, in which case the response deadline can be extended to 60 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 GDPR 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 deceased's 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 (except in circumstances where disclosure may prejudice the purpose of the exemption applied) and of their right to appeal.

2.3.3 Privacy Notices

It is the council's responsibility as a Data Controller, to tell customers how their information will be used. To achieve this 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
- the lawful basis for collecting the information
- whether the information will be shared and if so who with
- the rights of the Data Subject under GDPR and the Data Protection Act
- how long information will be held
- contact details for the council's Data Protection Officer
- their right to make a complaint to the Information Commissioner's Office and the contact details for the ICO

2.3.4 Amendments to Inaccurate Records

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 request that the processing of information about them be restricted or ceased if they believe the information to be inaccurate or being held unnecessarily. The council must investigate any such request and rectify if necessary. The Data Subject should be informed before any restriction is lifted.

2.3.5.1 Direct Marketing

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 and Assurance 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

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 of 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

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 the GDPR

Requests 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 GDPR. Any person who is unhappy with the way in which the council has handled their request may use this procedure.

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.

Under GDPR a customer has the right to make a complaint directly to the Information Commissioner's Office.

Part 3: Records Management Policy

3.1 Policy Statement

Walsall 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 the council 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 in accordance with the council's Protective Marking Procedure
- 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 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

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, directorates 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 Council's 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 Information Governance and Assurance Team 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.

The INSPIRE Regulations 2009 introduced a right to discover and view spatial datasets. This requires full metadata to be created for this information.

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 protectively marked either at the point of creation or receipt, and to carry that classification as a discrete marker. A report may have a header of 'OFFICIAL SENSITIVE' or a group email may carry a header of 'OFFICIAL'. In practice 'public' information classified as NOT PROTECTIVELY MARKED does not need to be marked as such.

Further guidance on the application of protective markers can be found in the Protective Marking Procedure.

When providing information to other public authorities it should be made clear what, if any, restrictions there should be on its usage and how it should be handled.

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.

Directorates should consult with the Information Governance and Assurance Team on the long-term storage or archiving of paper records and must use the council contact and 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 Information Governance and Assurance Team 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

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 Information Governance and Assurance Team 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

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.

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

All employees 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 GDPR states that information captured and retained must be accurate and up to date. All employees collecting or using personal data have a responsibility to ensure that this is the case.

It will be the responsibility of the Information Governance and Assurance Team 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.

Further guidance on Data Quality and the council's requirements in this regard are set out in the associated Data Quality Procedure.

3.3.11 Historical Records

The 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 council's archives serve can be found in the Archive Procedures.

Document History

Revision Date	Version	Revised By	Summary of Changes
11/02/2015	2.0	Caroline Hobbs	No amendments required. Version and metadata updated.
20/02/2016	2.1	Nailah Ukaidi	Slight amendments to roles and additional procedures no substantial updates
13/02/2017	2.2	Caroline Hobbs	Job titles, version and metadata only changed. No substantial updates
15/07/2017	2.3	Stephen Weaver	Update made to Records Management Policy to refer data quality procedure
05/03/2018	2.5 DRAFT	Paul Withers	Review to bring into line with ICO audit requirements and Legislative changes
	3.0	Paul Withers	Approved version.

Approvals

This individual Framework and Policies received the following approvals.

Name	Title	Signature	Date of Approval
Forum for Information Governance & Assurance (FIGA)			26/03/2018

The consolidated IG Policy Framework received the following approvals.

Name	Title	Signature	Date of Approval
Corporate Management Team (CMT)			00/04/18
Elected Members - Full Cabinet			00/04/18

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:

- HMG Security Policy Framework 2014
- General Data Protection Regulations (GDPR) 2016
- UK Data Protection Act 2018
- The Data Protection (Processing of Sensitive Personal Data) Order 2000
- Mental Capacity Act 2005
- 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.
- Caldicott Review 2017
- 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 2016
- International Standards for Information Security - ISO27001:2013 & ISO27002:2013
- Health and Safety at Work Act 1974
- International Standard for Information and Documentation, Records Management ISO 15489

- Records Management Code of Practice for Health and Social Care 2016
- Code of practice for legal admissibility and evidential weight of information stored electronically BIP0008:2014
- Common law duty of confidence
- Health and Social Care Act 2001
- ISO 27032:2012 Information technology Security techniques - Guidelines for cyber security
- ISO 27001 Information Security Management Standards
- PCI/DSS

Appendix 2 - Related Council Procedures and Guidance

- Procedure for Reporting and Managing Data Breaches
- 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
- Protective Marking Procedure
- E-mail & Internet Usage Procedure
- Handling Person Identifiable Data
- Information Classification Procedure
- Mobile Device Acceptable Use Procedure

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.

- Monitor the effectiveness of the Council's process for handling investigations and reporting incidents and breaches.

- Responsibility for approving procedures or plans, relating to Information Governance and ensuring that they are implemented.

- Responsibility for approving procedures or plans relating to Information Assurance to ensure that new or proposed changes to organisational processes or information assets are identified.

- Quality assure the work of the Information Management project and the Information Management / Governance Team beyond the life of the project.

- Identify risks relating to the management and use of information and work collaboratively to put in place measures to monitor and mitigate these.

- Ensures any actions or outcomes are shared accordingly with directorate leads, services and teams to provide assurance of clear communication.

Accountability

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

Meetings

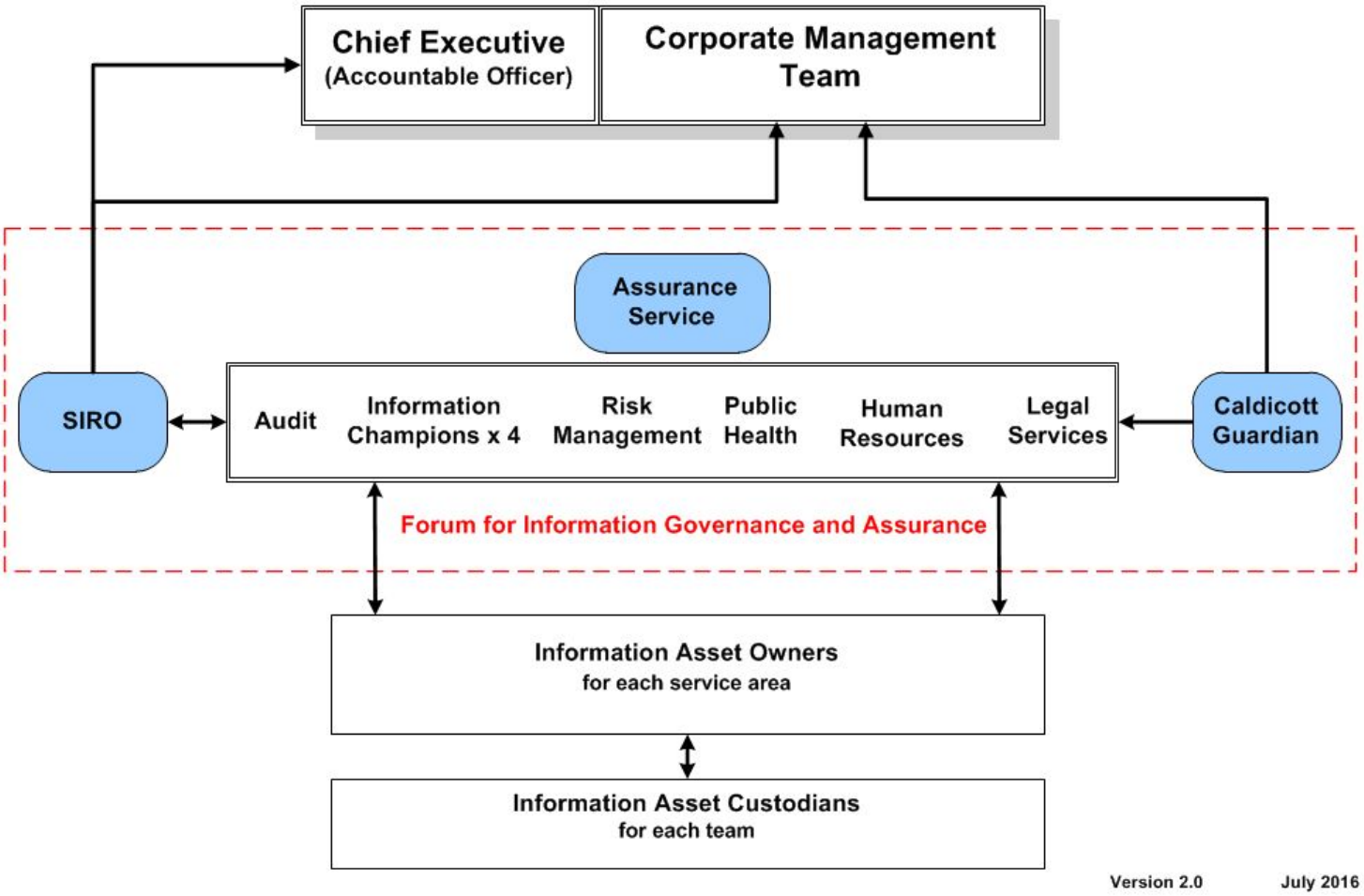
The group will meet at least 6 times per year. Decisions may be made outside of the physical board meeting via email confirmation.

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 in the diagram below; representation may also be required from other services as agreed by the Forum.

Governance Structure



Quorum & deputy arrangements

The quorum is reached when at least the following are in attendance:

Chair : IGAM, Caldicott Guardian or SIRO *and*

Information Champion Childrens or deputy *and*

Information Champion Adults or deputy *and*

Information Champion E&E or deputy *and*

Information Champion Change and Governance or deputy

A meeting that starts with a quorum present shall be not be deemed to have a continuing quorum in the event of the departure of any of the above unless an appropriate deputy remains throughout the duration, this is only relevant in the event of an important decision and is at the discretion of the Chair.

Deputies are required for all members of FIGA. *The information Champion deputy shall be an Information Asset Owner from the Directorate*

Appendix 4 - IG User Account Access Request Form

IG Request Form

For access to an individual's account

This form will help the Information Governance Team to determine the justified grounds for allowing access to a personal home drive, shared drive, email archive or email account.

It is vital that the Council undertake every possible measure to ensure the confidentiality and security of personal information and the rights of individuals. Therefore access to council wide accounts will only be granted where there is a justified and legal basis for doing so.

Depending on your completed form the Information Governance and Assurance Team may:

- Deny the request
- Insist that you take actions to ensure your services and teams follow business continuity requirements in sharing and storing business required data in an appropriate shared location with access controls to ensure business continuity in the event of unexpected absences.
- Apply other actions such as requesting an out of office be applied to the accounts to ensure business continuity rather than account access being granted.

This form must be completed by the senior manager and sent to the Information Governance and Assurance Team from an appropriate senior managers email account for validity.

In the sections below please supply the required level of information.

Please provide your contact details and the identification of the account in question.

General information	**Details:**
Name of the senior lead (First name. Surname)	
Contact email for the lead or manager	
Contact telephone number	
Name of the account for which access is required	
Name of the member of staff involved	

Please provide the details of the account or information types and conditions around this request

.

Purpose		**Details:**	
Identify the area or location of the information you require		Home drive	Yes/No
		Shared Drive	Yes/No
		Network area	Yes/No
		Personal Device	Yes/No
		Email Account	Yes/No
Please identify the grounds for requiring access		IG/DPA Breach	Yes/No
		Unauthorised access	Yes/No
		HR Investigation	Yes/No
		Code of Conduct	Yes/No
		Other	Please specify below
If you selected other as the ground for requiring access please give an explanation as to why you require access to the information		Details below:	
Please describe the information you require		Give detail - such as specific emails, dates sent, folder types and names or shared area link in the area below:	
Have you informed HR		Highlight the appropriate answer below	
		YES	NO
Have you informed the member of staff concerned		Highlight the appropriate answer below	
		YES	NO

Please return this form to InformationMgmt@walsall.gov.uk

Once we have assessed your request we will contact you to inform you of any further IG requirements:

Next steps may include:

- Contacting ICT to provide access or a copy of the information requested.
- Arranging for you or the appropriate lead to view the information in the prescience of an Information Governance and Assurance Officer
- Arrange for an appropriate HR lead to be present

Please remember that access to an individual's accounts and information can only be undertaken in the presence of an appropriate representative of the Council of Information Governance Team as this ensures the confidentiality and security of personal and private information for which you may not have a justified or lawful basis to access.

For internal IG use only

Actions	Yes	No	Authorised By
Approved			
Denied			
Referred to HR			
Viewing arranged			Date: