Data Security and Information Risk Policy

Version 2.0

Document Control

Organisation	Wigan Council
Title	Information Risk Policy
Prepared by	Executive Director – Business Support Services Service Director – Borough Solicitor
Owner	Senior Management Team
Subject	Information Security

Document Approvals

Version	**Sponsor Approval**	**Date Approved**
1.0	Chief Executive	SMT 24 August 2010
2.0	GDPR Working Group	

Document Distribution

Version	**Date Distributed**	**Distribution Method**
1.0	22 November 2010	LanConsent
2.0	Xxxxx	

Revision / Review History

Revision / Review Date	**Reviewer**	**Previous Version Ref**	**Description of any Revisions**
17.4.2018		1.0	2.0 Includes Elected members References GDPR throughout document 6.0 Provides a summary of obligations

Data Security and Information Risk Policy

1. Introduction (Why do we need this policy?)

Wigan Council seeks to maintain the highest standards of corporate behaviour and competence. In particular, it seeks to ensure that all its dealings with the public, staff, partners and stakeholders are conducted safely and fairly.

To assist with this, the organisation will develop clear and consistent guidance documents to fulfil all statutory, organisational and best practice requirements (see Appendix A).

This policy is an **Information Governance** document and forms part of the corporate governance arrangements of the Council. It sets out Wigan Council's approach to managing the risks which relate to collecting and storing information, much of which may be personal, sensitive or confidential. We are required by law and trusted by the public to keep this information secure, so a clear policy is needed to ensure consistent standards are maintained across all areas where information (paper based or electronic) is controlled or administered by the Council.

2. Purpose and scope (What is it about and who needs to read and adopt it?)

The purpose of this policy is to establish and explain your responsibilities as an employee and the rules of conduct for you as a member of staff regarding information risk management.

This policy applies to you if you work in Wigan Council whether operating directly or providing services to other organisations under a service level agreement or joint agreement. It will also apply to Elected Members of the Council.

What does this policy aim to do?

This policy is to help you know what to do to ensure that:-

- Information is protected against unauthorised access.
- Confidentiality of information is assured.
- Integrity of information is maintained.
- Regulatory requirements and legislation are met.
- Information technology systems operate in a manner that prevents the release of information (by accident or deliberate/criminal act), ensures their safe use and avoids damage to the specific system or any other system to which it is connected.
- Personal data (ie information that can be used to identify a person - including confidential and sensitive information about that person) and confidential business information is restricted to authorised users only.
- Business continuity plans are produced, maintained and tested.
- Appropriate information security and awareness training is promoted and made available to all staff.
- All breaches of information security, actual or suspected, will be reported to and investigated by appropriate officers within the Council and notified according to normal suspected irregularity procedures.

The lawful and correct treatment of personal information is essential to the successful delivery of all Council services and to maintaining public confidence in the Council.

3. Procedure – Information Risk Principles (What do I need to know?)

3.1 ~~.~~Managing An Information Handling Culture

It is the responsibility of the Council to establish and manage a lawful and effective information handling culture. Everybody needs to understand their responsibilities and how to safely handle data as they undertake their daily tasks, regardless of seniority.

Everybody needs to acknowledge that information is valuable and must be protected, risks must be mitigated. Everybody must demonstrate through their decisions and actions, the importance of effective handling of information, viz.:-

- Everybody should appreciate that good information handling is integral to their job.
- Managers should adopt these principles and lead by example on maintaining effective and agreed risk controls.
- Everybody should be able to answer general questions about information protection policies and procedures, and make informed information risk decisions for themselves including knowing the limits of their competence and when to refer to Management for guidance.
- All Employee Development Review development plans will include competencies on information handling.

It is the responsibility of the Strategic Management Team (SMT) to ensure that the Council has an open and effective approach to information incidents and learning.

Everybody should be encouraged to question instructions that seem inappropriate and may pose a risk to our information and be encouraged to report any instances of inappropriate behaviour.

Our customers have a right to know that we take good care of the information they provide us with to deliver services. If you fail to comply with this policy there could be a significant effect on the efficient operation of the Council and it may result in loss of trust, financial loss, reputational damage, and an inability to provide services to the Council's customers. It could also result in you being held personally liable for the loss of information under the General Data Protection Regulation.

3.2 ~~.~~Information Risk Management

Information Risk Management must be embedded within the Council's overall risk management processes within Strategic and Departmental Risk Registers.

The Council's policy and associated processes in respect of Information Risk are part of the overall assurance framework and will be reported annually within the Council's Statutory Annual Governance Statement.

4. Duties and Responsibilities (Who is involved in implementing this policy?)

Cabinet

Cabinet has overall responsibility for the strategic management and effective governance of all the Council's services and the preparation and adoption of all Council plans, policies and strategies that are not included in the Policy Framework or the Budget.

Accordingly, Cabinet is responsible for the strategic context in which organisational process documents are developed, and for establishing a scheme of governance for the formal review and approval of such documents.

Strategic Management Team (SMT)

The Strategic Management Team collectively own the Information Risk Policy and are responsible for ensuring all aspects of its implementation, both from a corporate perspective and within their respective departments.

The Senior Information Risk Officer (SIRO) is responsible for developing this policy and for reviewing it regularly to ensure that it remains appropriate to the business objectives and the risk environment. The policy should be published and communicated in a manner that is relevant, accessible and understandable to all employees and relevant external parties, including delivery partners.

Senior Information Risk Owner (SIRO)

The Council has assigned a Senior Information Risk Officer (Executive Director – Business Support Services) who has the responsibility for providing SMT and the Council with the details of Information Risk.

The SIRO is responsible for:-

- Ensuring, through SMT, that an overall culture exists where everybody values and protects information within the organisation.
- Developing the organisation's overall Information Risk Policy and risk assessment process, testing its outcome and ensuring that it is used.
- Advising the Chief Executive on any information risk aspects and reporting annually within the Council's Annual Governance Statement.
- Owning the organisation's Information Risk Recovery Plan and ensuring corporate learning arises from any incidents.

Assistant Director Strategic ICT Partnerships

The Assistant Director Strategic ICT Partnership ~~s~~has responsibility for providing a safe ICT environment for the storage of our information: -

- Maintaining secure ICT systems with appropriate levels of security and access controls to prevent accidental or unauthorised disclosure of information.
- Advising users on technological solutions to help minimise information governance risks.
- Review all identified ICT information risks with information asset owners to support the maintenance of the Council's Strategic Information Governance Risk Register.
- Communicating identified risks and their assessed impacts on the Council and recommending mitigation action to the SIRO.

Executive Directors

Each Executive Director will be designated with overall Risk/Data Ownership for information assets under their control at Directorate level. Through their departmental structures, they will in turn identify a Business Manager (Information Asset Owners) at Service Director or Head of Service Level. Each Information Asset Owner is responsible for *"operationally owning the information contained in their systems".*

Each Executive Director is responsible for ensuring that all staff within their respective departments are informed of and receive the necessary training to enable them to comply with this policy in maintaining appropriate levels of information security and awareness.

Line Managers

- Managers are responsible for ensuring that current staff and any new staff are aware of and understand this policy. They should discuss the policy with teams during briefing sessions and with new starters at induction.
- It is the responsibility of every line manager to ensure that they and their staff adhere to the terms of this policy.
- When a line manager suspects anybody may be breaching the Information Security policy, they must inform the respective Service Directors or Head of Service and request an initial investigation.

Everybody

All staff, including temporary and agency staff, are responsible for:-

- Keeping safely any information with which they have been entrusted. This includes usage, storage and any onward communication of the information. Unauthorised breaches or disclosures can be a criminal offence and could result in disciplinary action being taken or even prosecution.
- Co-operating with the development and implementation of policies and procedures as part of their normal duties and responsibilities.
- Identifying the need for a change in policy or procedure as a result of becoming aware of changes in practice, changes to statutory requirements, revised professional standards and local/national directives, and advising their line manager accordingly.
- Identifying training needs in respect of policies and procedures and bringing them to the attention of their line manager.
- Attending training / awareness sessions when provided.

5. Implementation (How will people be made aware of this policy?)

This policy will be issued by Net Consent to all officers and will be posted on the Council website. In addition the policy will be subject to wide ranging publicity in consultation with the Council Media Team.

Executive Directors will ensure that appropriate arrangements are in place to:-

- satisfy themselves that this document has been cascaded to appropriate staff,
- safeguard any information held within their service, and
- identify any training required by their staff to reach the specific competencies identified in this document.

All Managers will be responsible for ensuring that relevant staff within their own departments / sections have read and understood this document and are competent to carry out their duties in accordance with the procedures described.

6. Summary of obligations

The fundamental principle of this policy is that personal data must be processed and stored securely pursuant to the requirements of the General Data Protection Regulation, ~~In~~in practice this means**:**

All users of council information are required to ensure that they:

- Familiarise themselves with, and adhere to, this and all other council information security policies
-Only access information needed for their legitimate duties
-Access information only when authorised by their line manager
- Protect the confidentiality, integrity and availability of the council's information, wherever the information is located
-Safeguard their network account, passwords, any physical token used to access systems and ID cards used to access rooms/buildings
-Securely destroy all confidential information before discarding, whatever its format
- Report all actual or suspected information security breaches to ICT Services and their line manager (where appropriate). This can be done anonymously or otherwise using the form on the ICT Help Desk page on the intranet

The obligation to protect confidential information continues after a user leaves the council or no longer has cause to access council information.

In addition to the requirements listed above, managers must:

- Ensure their staff are aware of their responsibilities regarding information security and conform to this, and all other council information security policies
- Ensure their staff can only access information needed for their legitimate duties
- Ensure that departmental procedures support this policy
-Employ control procedures to eliminate/minimise the risk of unauthorised access, fraud, theft or disruption to services
-Ensure that all procedures are effectively communicated to those who use, administer, process, share or transport confidential information in any form, physical or electronic
- Report all actual or suspected information security breaches to ICT Services and co-operate fully

Appendix A

Legal Principles

Data Protection Principles

The General Data Protection ~~Regualtion~~Regulation Principles states that personal information:-

- Processed fairly, lawfully and in a transparent manner in relation to the data subject.
- Collected for specified, explicit and legitimate purposes and not further processed for other purposes incompatible with those purposes.
- Adequate, relevant and limited to what is necessary in relation to the purposes for which data is processed.
- Accurate and, where necessary, kept up to date.
- Kept in a form that permits identification of *data subjects* (Usually members of the public) for no longer than is necessary for the purposes for which the personal data is processed.
- Processed in a way that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Caldicott Principles

The Caldicott report outlines six principles:

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

Principle 2 – Only use it when absolutely necessary.

Principle 3 – Use the minimum that is required.

Principle 4 – Access should be on a strict need-to-know basis.

Principle 5 – Everyone will understand his or her responsibilities.

Principle 6 – Understand and comply with the law.