WIRRAL

Information Governance Policy

INFORMATION GOVERNANCE POLICY DETAIL

Contents

1 Policy Statement

Information is a vital asset. It is essential in-service delivery, service planning and performance management.

In holding, managing and using that information, Wirral Borough Council (the Council) recognises the need for an appropriate balance between its obligations of openness, such as those under the Freedom of Information Act 2000, and of confidentiality, such as under the Data Protection Act 2018 and EU General Data Protection Regulation 2016.

The Council will have a suite of policies, supported by the necessary processes and communication, to enable it to meet those obligations.

The Council will follow Government[1] best practice and guidance and will comply with the requirements of the NHS Data Security and Protection Toolkit to demonstrate it is properly managing its, and its citizens', information.

This policy will be a point of reference for staff so they know what they should and should not do when handling information.

2 Background

Information Governance (IG) covers a broad spectrum of disciplines, responsibilities and skillsets. It includes creating, communicating, storing, using and distributing the information it needs to deliver its services and corporate objectives. It covers all information in all formats - paper, electronic (including graphical, audio and video files) and, so far as feasible, that which is held in people's heads.

Failure to manage information properly exposes the council to a significant financial, legal, public relations and potentially manpower-shortage risks. By putting in place the proper policies, frameworks, technology and training, the Council will minimise those risks, maximise potential and promote a culture which recognises and meet its information governance principles. This document states the Council's policies to achieve those goals.

The Information Governance Management Framework describes how IG will be managed and where responsibilities sit within the Council.

Within the IG Management Framework, the Information Governance Board will be responsible for delivering the IG Policy.

Wirral Borough Council's Information Governance documentation is made up of four basic tiers:

- ➢ Information Governance Principles
  - ➢ Information Governance Management Framework
    - ➢ **Information Governance Policy: covering the breadth of IG – this document**
      - ➢ Suite of procedures, guidance and tools to implement IG Policies.

This policy exists to state what the Council will do to meet its obligations as a custodian of people's information. Those obligations come from:

- Data Protection Act 2018
- EU General Data Protection Regulation 2016
- Human Rights Act 1998
- Freedom of Information Act 2000
- Environmental Information Regulations 2004
- Copyright, Designs and Patents Act 1988
- Local Government Acts 1972 – 2003
- Electronic Communications Act 2000

[1] National Cyber Security Centre

- Regulation of Investigatory Powers Act 2000
- Misuse of Computers Act 1990
- Consumer Protection Regulations 2000
- The Electronic Commerce Directive 2000
- Re-use of Public Sector Information Regulations 2015

This policy will reduce the risk of information misuse. However, the policy will also be evidence of proper information governance and in the event, albeit reduced likelihood, of an incident will help mitigate criticism and legal action. That will require the policy to be properly supported and communicated.

3 Policy Approach

The policies laid out in this document cover the range of IG requirements. They are split into logical sections to aid access by their respective target audience as, while all staff should comply with all Council policies, some are not meaningful to some staff.

The policy sections are:

> **4) Confidentiality and Data Protection**: this section is primarily about users and their legal responsibilities. It includes adherence to the Caldicott Principles, training and how staff are made aware of their responsibilities, thus avoiding vicarious liabilities.
>
> **5) Information Security:** this section is mainly about the IT aspect of ensuring security is assured, but also covers paper-based **systems**. It covers the policies that govern how IT systems and paper-based information resources are looked after and their security assured.
>
> **6) Information Assurance:** this section covers the information **content**. How information is collected and managed to ensure it is accurate and used effectively and appropriately.

4 Confidentiality and Data Protection

4.1 Caldicott Guardian Policy

The Caldicott Guardian acts as a conscience in matters of data confidentiality and sharing. They work as part of a broader Information Governance function within the Council.

The Council's Caldicott Guardian will:

- Be a senior person within the Council's social care management team
- Be a senior social care professional
- Act as a champion for data confidentiality at Directorate Management level and as part of the Council's Information Governance Board.
- Provide confidentiality and data protection expertise
- Ensure that confidentiality issues are appropriately reflected in organisational strategies, policies and working procedures for staff
- Oversee all arrangements, protocols and procedures where confidential social care information may be shared with external bodies including disclosures to other public sector agencies and other outside interests

4.2 Department/Managers' Responsibilities

Proper Information Governance is the responsibility of every Council member of staff. A range of policies and procedures are in place to support them in meeting that responsibility.

The onus for discharging that responsibility will be with managers.

It is the role of Departmental managers to ensure that staff and, where relevant, third parties achieve a level of awareness of Information Governance issues relevant to their roles within the

Council, and continue to have the appropriate skills and qualifications to ensure security is maintained.

Managers will assure Cabinet, corporate senior management and Chief Officers through the Information Governance: Department Assessment Process that the Council's IG policies and procedures are being followed and that their departments are looking after people's information properly.

Line managers will ensure that users return all of the organisation's assets in their possession upon termination of their employment, contract or agreement. This includes recovering any copies of information in any format.

4.3 Human Resources Security Policy

The Council understands that to reduce the risk of confidentiality breaches, theft, fraud or inappropriate use of its information systems anyone that is given access to Council information and information systems must be suitably trained and qualified for their role; they must fully understand their responsibilities for ensuring the responsibilities for ensuring the security of the information; they must only have access to the information they need; and this access must be removed as soon as it is no longer required.

The Council will ensure that:

- Security and confidentiality roles and responsibilities of employees, contractors and third party users will be defined and documented within their respective job descriptions, contracts, terms and conditions, codes of conduct or any other relevant document defining their role and relationship with the Council.
- Users have appropriate IG training for their role (as determined by the point above).
- Individuals are checked to ensure that they are authorised to access Council information systems. This will be done as part of the Council's HR Policy.
- Users are trained to use information and information systems securely.
- User access to information systems is removed promptly when the requirement for access ends.
- The Employee Code of Conduct will state the the employee's and any other user's legal responsibilities and rights, e.g. regarding copyright laws or Data Protection legislation.

4.4 IG Training Policy

Staff will be given the knowledge they need to look after the Council's information properly.

Each Council job role will be assessed to identify the necessary IG training requirements required for the job based on what confidential information the role handles or may reasonably come into contact with.

Suitable training will be given to each person based on the role or job they do.

4.5 Data Protection Policy

The Council has a separate Data Protection Policy approved by Council that is published on its public website.

The Data Protection Policy is designed to ensure that the confidentiality of personal data is maintained and to increase the access given to individuals to information relating to them.

The Data Protection Policy is designed to complement other Council policies, which relate to personal data, including this IG Policy.

4.6 Information Sharing Policy

To deliver services effectively the Council needs to share personal information with its partners. To ensure such sharing is done securely and appropriately the Council will cooperate with its partners in developing and implementing suitable Information Sharing Agreement (ISAs) processes

The Council’s Caldicott Guardian will be a key signatory to ISAs and processes – see section **4.1 Caldicott Guardian Policy.**

4.7 Third Party Procurement Policy

Third Party Information Security covers any person or organisation doing work for the Council (e.g. volunteers, contractors or through third parties).

Third parties processing or accessing Council systems and information present a risk to the Council’s obligations as a custodian of information. These risks need to be mitigated through appropriate controls:

- All procurements will follow the Council's procurement guidelines and policies.
- The Council’s standard terms and conditions for service provision will include necessary terms to hold third party service providers accountable for Data Protection and Duty of Confidentiality obligations.
- Employees of service providers who may have access to confidential information will have had the necessary DBS checks. This will be a condition of the service provider’s contract.
- Any service provider processing personal information on behalf of the Council will have the necessary Data Protection Act / General Data Protection Regulation Data Processing clauses in their contract.
- Any person who is not an employee but is engaged in doing work for the Council who may have access to confidential information, paper or electronic, must sign the Council’s Confidentiality Code of Conduct and be made aware of the Council’s IG Policy and appropriate supporting procedures and processes.

5 Information Security

5.1 Asset Management Policy

The purpose of this policy is to achieve and maintain appropriate protection of organisational information assets. It does this by ensuring that every information asset has an owner and that the nature and value of each asset is fully understood. It also ensures that the boundaries of acceptable use are clearly defined for anyone who has access to the information.

This policy applies to all the systems, people and business processes that make up the Council’s information systems.

The Council will create and maintain a register of its information assets, such as:

- filing cabinets and stores containing paper records
- computer databases
- data files and folders
- software licences
- physical assets (computer equipment and accessories, PDAs, cell phones)
- key services
- key people
- intangible assets such as reputation and brand

5.1.1 Critical Assets

Critical assets will be identified and have an information asset owner (IAO) assigned to them. An IAO must be a member of staff whose seniority is appropriate for the value of the asset they own. The owner’s responsibility for the asset and the requirement for them to maintain it should be formalised and agreed.

5.1.2 Unclassified and trivial information assets

Items of information that have no security classification and are of limited or no practical value should not be assigned a formal owner or inventoried. Information should be destroyed if there is no legal or operational need to keep it and temporary owners should be assigned within each department to ensure that this is done.

5.1.3 Information assets with short term or localised use

For new documents that have a specific, short term, localised use, the creator of the document will be the asset owner. This includes letters, spreadsheets and reports created by staff. All staff must be informed of their responsibility for the documents they create.

5.2 **Information Security Governance & Risk Management Policy**

The Council will implement and maintain an information Risk Management framework.

The Information Security Governance and Risk Management Framework will:

- Complement and adhere to the Council's Risk Management Policy.
- Set down processes for mitigating identified risks to an acceptable level.

The Senior Information Risk Officer (SIRO) will be responsible for information risks. Information Asset Owners (IAOs) will be responsible for reporting risks relating to their assets to the SIRO.

5.3 **Access Control Policy**

Access to Wirral Council's information and ICT systems must be protected. Whilst different business applications have varying security requirements, these individual requirements must be identified through risk assessments that will control the access to them.

Access controls are put in place to protect information by controlling who has the rights to use different information resources and by guarding against unauthorised use. Formal procedures control how access to information is granted and how such access is changed.

This policy also mandates a standard for the creation of strong passwords, their protection and frequency of change.

5.4 **Policy on Use of Network Services**

To reduce the risk of confidentiality breaches, theft, fraud or inappropriate use of its information systems, access to Council information and information systems will:

- Be determined by a person's role – be that Council employed, a volunteer or third party employed.
- Only be to access the minimum person identifiable information they need for their role.
- Be given the appropriate training, guidance and tools for them to fully understand their responsibilities for ensuring the security of Council information.
- Be removed as soon as it is no longer required, for instance when they leave their role (in some cases this will be if the person is suspended for any reason).
- Be only given to those employees who have been recruited using the HR Council's HR Policies on identity, right of employment and appropriate DBS checks

  OR
- Be only given to third parties (e.g. contractors, contracted company employees, volunteers, and agency staff) who have been appointed subject to the Council's Procurement guidelines and policies and have signed a Confidentiality Code of Conduct.

5.5 Password Policy

The purpose of this policy is to mandate a requirement for the creation of strong passwords, their protection and frequency of change.

All users of Councils systems will

- Create and maintain a strong password as dictated in the Council's Information Security Password Standards.
- Change their password as directed by ICT – see the Council's Information Security Password Standards.
- Keep their password confidential, keep it secure and not share it with anyone.

5.6 IT Communications & Operations Management Policy

The Council's infrastructure will be kept secure by ensuring appropriate IT security controls are in place. ICT will be responsible for putting in place security processes that meet the requirements of the PSN and are recognised IT industry good practice, including:

- Providing users with the facilities and opportunities to work remotely in ways that maintain the confidentiality, availability and integrity of council information and information systems.
- Ensuring that all users who work remotely are aware of the Mobile Working Standards[2] which govern the use of mobile computer devices and remote working opportunities.
- Laptops and portable devices will be suitably encrypted.
- Removable media, such as USB memory sticks, will only be usable if encrypted to standards specified by ICT.
- ICT will ensure they have in place a patch management process to keep operating systems and software up to date.
- All Council IT equipment will have up to date anti-virus software installed and running as specified by ICT.
- Staff and Councillors will be able to access the internet using Council IT equipment subject to the IG Policy and Summary Code of Practice.
- Staff and Councillors will not download or install software without approval of ICT.
- ICT will operate an industry standard Change Control[3] process (such as ITIL) to minimise the risk of disruption from IT infrastructure changes.
- As part of the change control process all Council departments will consult ICT for approval of any IT hardware or software purchase or installation that will connect to the Council's IT Network. Information Systems Acquisition, Development and Maintenance Procedures[4]
- The use of personal computing devices to access Council information and ICT systems is permitted subject to certain conditions. These conditions include policy and technical measures to ensure the confidentiality, availability and integrity of Council information is maintained.

New systems and development of systems will be undertaken in a consistent way that ensures compliance with security information standards.

ICT will be consulted on all Information and IT system procurements and developments to ensure security standards are maintained.

[2] Information Responsibilities, see section Mobile Working

[3] See link to Change Control Procedures

[4] See link to Systems Acquisitions and Development

5.7 Information Security Incident Management Policy

The definition of an incident is an adverse event that has caused or has the potential to cause damage to an organisation's assets, reputation and/or personnel. Incident management is concerned with dealing quickly and effectively with intrusion, compromise and/or misuse of information or information resources, and risks to the continuity of critical information systems and processes.

The Council will ensure it has in place procedures for investigating and assessing incidents and risks by a suitably qualified information security advisor.

The Council will use the NHS Data Security and Protection Toolkit (DSPT) Serious Incident Requiring Investigation (SIRI) tool, which is endorsed by the ICO, to categorise incidents and inform when they should be notified to the ICO.

Staff will be made aware of the processes for raising alerts of incidents or risks. Managers will be responsible for ensuring staff are aware of and follow these processes.

As part of a continuous process to reduce risks of incidents, the causes of information incidents and the effectiveness of mitigations will be reviewed afterwards.

5.8 Physical and Environmental Security Policy

All Wirral Council employees, contractors and users are responsible for ensuring the safety and security of the council equipment and information (including both electronic and paper records) that they access or use. This includes the physical and environmental security of the council's information and information systems.

The Physical and Environmental Security Standards[5] will be applied to all information and systems to provide the protection appropriate to the level of information held and the business impact of unauthorised access.

Each department is responsible for assessing the level of protection required for their teams, sections and locations and implementing the required security standards.

5.9 Business Continuity Management (BCM) and Disaster Recovery (DR) Policy

The Council has a Business Continuity Policy. From an IG perspective BCM and DR presents risks to information. The organisation needs suitable controls in place to mitigate those risks, including:

- All information systems will have a regular back up routine agreed between the asset's IAO and ICT.
- All information systems will have a restore regime agreed between the IAO and ICT.
- Key systems will have disaster recovery processes agreed between ICT and their IAO.
- Processes for checking data integrity will be implemented, particularly for key systems, to check for corruption in the event of system failures or downtimes.
- Processes for updating records, e.g. manual entry of paper records, will be developed for recovering from system downtime to ensure records remain complete and accurate.

5.10 Email Policy

Email has become an important part of the recording of decisions within the Council and hence much of the Corporate Memory is stored there. It is important that the email lifecycle is correctly and securely managed.

- Email will be treated as a business communication and not an ephemeral tool. Council email is not a personal private email account.

[5] Information Responsibilities, see section Physical and Environmental Security

- All Councillors and staff will be trained in email management. Guidance will be given to staff and Councillors individually and also on the Intranet.
- All Councillors and staff must manage their emails as they would their documents.
- Emails will be deleted after two years.
- If they are needed as records and therefore need to comply with different retention and disposal schedules then they must be moved and saved out of MS Outlook.
- All email users will use email securely:
- They will not download emails with confidential information to insecure IT equipment, such as user non-work computers.
- They will only send emails containing confidential information via secure means or only to other internal email accounts (see Digital secure email guidance).

5.11 Payment Card Policy

The Council receives payments for services via a number of channels, e.g. Face-to-Face, by phone and online. Payment Cards, i.e. Credit and Debit cards, are a convenient way to pay but the Council must ensure that Cardholder data is protected against the risk of financial, or other, fraud.

The Council complies with the requirements of the Payment Card Industry Data Security Standard (PCIDSS).

The Council will:

- Only implement card payment solutions which are accredited against the relevant Payments Card Industry Security Standards Council standard.
- Maintain a register of all card payment devices.
- Periodically inspect all card payment devices for signs of tampering.
- Promptly report any loss, damage or suspected tampering of any card payment device to the appropriate bodies, eg device supplier, payment solution provider.
- Provide appropriate training to all staff who handle card payments.
- Maintain continuous PCI DSS accreditation of all Council systems which accept payment by card.

6 Information Assurance

6.1 Data Quality Policy

Data Quality is an integral part of performance management and decision-making. The Council will implement policies and procedures to support its Performance Policy This is to ensure data is

- **Complete** gives the whole picture.
- **Accurate** provides an honest reflection of performance.
- **Valid** conforms to definition.
- **Reliable** trusted and collected consistently.
- **Relevant** applies to the situation in which it will be used.
- **Timely** available for intended use within a reasonable time period

To achieve this:

- All staff will receive training and guidance to ensure they have an understanding of the importance of data recording, making amendments and the implications of failing to do so, including possible adverse impact upon the service user (e.g. confidential information or appointments going to the wrong address).

- No user will be allowed to record data without the proper training.
- Data will be checked with service users for updates and accuracy whenever the service user presents.
- Routine audit and monitoring will be undertaken to ensure the procedures and processes in place for checking and correcting service user records are effective.
- Data reconciliation processes will be established to ensure data in disparate systems that is meant to be identical is actually identical: such as a service user's data of birth.
- New systems and system changes will comply with the Council's data standards and reporting requirements.
- National data standards will be used where they are applicable.

6.2 NHS Numbering Policy

The NHS Number is the national unique patient identifier that makes it possible to share patient information across the whole of the NHS and Local Authorities (in a Health and Social Care context) safely, efficiently and accurately.

It has now become a central policy imperative that Local Authorities move towards using the NHS Number as the primary identifier across all Children's Services, Adult and Disability Services, and Public Health populations. This is in line with the criteria set out in, amongst others, the Better Care Fund.

The Council will ensure:

- That service user records, both paper and electronic, have an NHS Number stored on them as early as possible in the episode of care. Where a local identifier is used this must be in addition to and not instead of the NHS Number.
- Staff use the NHS Number in internal communications to identify the service user and to link records together.
- Correspondence between health and social care use the NHS Number as primary identifier.
- The service user is aware of the NHS Number, for instance including it in any letters or forms for the service user.
- All new systems and software upgrades have the NHS Number built in as the primary identifier.
- It puts in place a strategy for implementing the NHS Number across relevant systems.

6.3 Pseudonymisation

The Data Protection Act 2018, EU General Data Protection Regulation 2016, the Human Rights Act 1998 and the common law relating to confidentiality require that the minimum personal data are used to satisfy any particular purpose, that organisations respect people's private lives unless there is a lawful exemption and that information obtained in confidence should not normally be used in an identifiable form without the permission of the service user concerned.

The underlying principle is to ensure, as far as is practicable, that individual service users cannot be identified from data that are used to support purposes other than their direct care or to quality assure, such as with care audits, the care provided.

This means that when person identifiable information is used for other purposes it should be de-identified as much as possible.

The Council will follow the ICO's Anonymisation Code of Practice. It will:

- Ensure that relevant staff are aware of and trained to use anonymised or pseudonymised data.
- Ensure that organisations from which Social care and services are commissioned also comply with the necessary de-identifying processes.
- Ensure appropriate changes are made to processes, systems and security mechanisms in order to facilitate the use of de-identified data in place of person identifiable data.

6.4 **Records Management Policy**

The Council's Records Management Policy defines records management as the process whereby an organisation manages its records, whether created internally or externally and in any format or media type, from their creation or receipt, through to their disposal or permanent preservation within Wirral Archives Service

The Council Records Management Policy is a separate policy that is approved by cabinet. It is mentioned in this policy for the sake of completeness.

6.5 **Corporate Retention and Destruction Policy**

The Council's Corporate Retention and Destruction Policy details recommended retention periods for records created and maintained by Wirral Council. It lists the types of records created or received by Wirral Council, and the length of time they should be retained, in line with business need, legislative, statutory and regulatory requirements. The Policy refers to all records, regardless of their format. It includes both paper and electronic records.

The Council Corporate Retention and Destruction Policy is a separate policy that is approved by cabinet. It is mentioned in this policy for the sake of completeness.

7 Responsibility for Work Equipment

The meaning of 'work equipment' is extremely wide. It covers almost any equipment used at work and includes computer equipment such as workstations, laptops, PC Tablets, phones, etc. Such equipment can be expensive and difficult to replace. When using Council equipment all employees are expected to exercise a duty of care towards equipment and follow all operating instructions, safety standards, and usage guidelines when using any equipment. The improper or negligent use of Council equipment by employees can result in disciplinary action

8 Commitment to Equality

Please identify which, if any, of the following Equality Duties this policy addresses:

Eliminate unlawful discrimination, harassment and victimisation	To advance equality of opportunity	To foster good relations between different groups of people
□	□	□

While this policy has no direct implications for equality and diversity, protection of sensitive data supports equality by preventing access to information that could be used for discrimination.

9 Related Policies

The IG Policy is linked to the following Council policies:

- Corporate Governance Policy
- Risk Management Policy
- HR Policies
- Employee Code of Conduct
- Performance Management Framework
- Corporate Retention and Destruction Policy
- Records Management Policy
- Wirral Council Business Continuity Policy

10 Consultation

There is no consultation required with staff, Trade Unions or the public, but communication of the Information Governance policy to staff is essential to its success.

11 Communication and Awareness

This policy is considered:

Internal	External
[For Members, Officers and Contractors]	[For our Residents, Customers and Service Users]
☑	□

The policy will be published on the Council's Intranet. It will be incorporated in the Performance Appraisal process.

12 Monitoring and Review

The tables below set out the ownership and review schedule for this document. The Information Governance Policy document will be reviewed **every two years** as part of the Information Governance Policy and Guidance Review Programme. However it may be necessary to review as and when required, for example, due to legislative changes or if an issue arises around its effectiveness.

Document Ownership	
Document owned by:	**Senior Information Risk Owner**
Document written by:	**Patrick Reed**
Date document written:	**April 2014**
Document last amended:	**February 2020**
Document due for next review:	**February 2022**
Document reviewer:	**Information Governance and Security Officer**

Version Control Table:
All changes to this document are recorded in this table

Date	Notes/Amendments/Approval	Officer
4 May 17	Transferred to standard template. Reviewed for currency	Judith Barnes, Information Governance and Security Officer
14 Dec 17	Altered to include reference to EU General Data Protection Regulation.	Judith Barnes, IG&SO
1 Mar 18	Amended for style and minor content changes	John D Williams / Judith Barnes
4 Feb 20	Payment Card Policy added and minor updates	Judith Barnes

Appendix 1 – Legislation involved in Information Governance and Data Protection

Data Protection Act 2018

EU General Data Protection Regulation 2016

Human Rights Act 1998

Freedom of Information Act 2000

The Environmental Information Regulations 2004

Copyright, Designs and Patents Act 1988

Local Government Acts 1972 – 2003

Electronic Communications Act 2000

Regulation of Investigatory Powers Act 2000

Computer Misuse Act 1990

Consumer Protection Regulations 2000

The Electronic Commerce (EC Directive) Regulations 2002

The Re-use of Public Sector Information Regulations 2005

Appendix 2 – Processes and Procedures

The following documents and resources provide supporting guidance on the policies contained in this document.[i]

Confidentiality and Data Protection

Caldicott Policy

Department/Managers' Responsibilities

Human Resources Security Policy

Information Security Training

Data Protection Policy

Information Sharing Policy

Procurement Policy and Procedures

Information Security Dos and Don'ts

Information Asset Management Policy

Information Risk Management

Access Control Policy

Policy on Use of Network Services

Password Policy

IT Communications & Operations Management Policy

Information Security Incident Management Policy

Physical and Environmental Security Policy

Business Continuity

Secure Email

Data Quality

Corporate Retention and Destruction Policy

[i] The Council's policies and guidelines can be accessed via the intranet links: What do I need to know and Responsibilities for Information.