CITY OF WOLVERHAMPTON COUNCIL

Information and Cyber Security Policy

IS00

wolverhampton.gov.uk

Version History

Version	Date	Description	Author, Role
0.1	19/12/12	First Draft	Anna Moore
0.2	12/02/13	Amended to increase emphasis on all information not just ICT based.	Anna Moore
0.3	27/03/13	Revised following audit review	Anna Moore
0.4	12/04/15	Revised following IGB consultation	Anna Moore
0.5	23/04/15	Revised to take account of cyber risks	Martin Eades
0.6	16/08/16	Revisions approved by SEB	Martin Eades
0.7	23/05/18	Revised to take account of GDPR	Martin Eades
0.8	05/07/19	Annual Review	Stuart Taylor
0.9	21/09/21	Review following restructure of IG policy framework	IG Team
0.10	10/11/21	Review by Digital and IT Management Staff	Jai Ghai, Ismail Patel
1.0	17/02/22	Approval by members of the IG Board and SEB	IG Team
2.0	05/12/23	Scheduled review	IG Team

Table of Contents

Introduction 3

Legal and Regulatory Obligations for the Council 3

Scope 4

Strategic Approach and Principles 4

Key Elements of Information and Cyber Security Policy Management 5

Risk Management 6

Engagement and Training 6

Asset Management including information handling and protective marking 7

Architecture and Configuration 9

Vulnerability management, Logging and Monitoring 10

Identity and Access management 10

Data Security 10

Incident Management 11

Supply Chain Security 11

Roles and Monitoring 12

Training and dissemination 13

Links to other Policies 13

Introduction

City of Wolverhampton Council (CWC) is making increasing use of a range of information, including service user information, held by the Council and other public and private sector organisations in order to ensure the continued delivery of services. In addition, the Council is making increasing use of Digital Technologies to manage this whilst still continuing to hold and maintain a significant quantity of paper-based information and records.

The information that the Council holds, processes, maintains and shares is an important asset that, like other important business assets, needs to be suitably protected.

In order to build and maintain public confidence and ensure that the Council complies with relevant statutory legislation, it is vital that CWC upholds the highest standards of information security and has policies to support and maintain these standards.

Information and cyber security are a key area in the Council's overall information governance management framework that covers the wider requirements of information management, including records management and data quality.

The purpose of this policy is to ensure the highest standards are maintained across the Council at all times so that:

- The public and all users of the Council's information are confident of the confidentiality, integrity and availability of the information used and produced.
- Business damage and interruption caused by cyber security incidents are minimised.
- All legislative and regulatory requirements are met.
- The Council's information is used responsibly, securely and with integrity at all times and that this applies to manual and electronic information.

This policy also sets out the overall objective and principles underlying Information and Cyber Security at CWC and specifies the management arrangements and key responsibilities.

Legal and Regulatory Obligations for the Council

The Council's statutory obligation to have sound information and cyber security arrangements in place originates in the UK General Data Protection Regulation 2016/679 (UK GDPR), which states in Article 5, 1. (f): "processed in a manner 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 ('integrity and confidentiality').

The Council depends on the confidentiality, integrity and availability of its

information and Digital Technologies to such an extent however, that a serious breach of information security could impact on the Council's ability to deliver a wide range of statutory services.

The Council also has to be seen to be 'considering whether IT equipment available to the general public should use filtering solutions that limit access to terrorist and extremist material' under the Prevent Duty, brought in as part of the Counter-Terrorism and Security Act 2015.

In addition, the Council has contractual obligations to ensure sound security if it is to use the Government Public Services Network (PSN); use secure connection with the National Health Service; comply with the requirements of Cyber Essentials Plus; meet Payment Card Industry Data Security Standards (PCI DSS) or receive or share information with partner agencies under information sharing arrangements.

Scope

This policy applies to all information held or owned by CWC, any Digital and IT equipment and infrastructure used, and the physical environment in which the information and/or supporting IT is used. This policy applies to any person that requires access to Council information systems or information of any type or format (manual or electronic).

This policy will apply to anyone accessing or using Council data, including for example: employees, temporary or contract staff, volunteers, work placements, council members, contractors, suppliers, services providers, or other partner agencies.

Where access is to be granted to any third party (e.g., contractors, service providers, voluntary agencies, and partners) compliance with this policy must be agreed and documented.

Strategic Approach and Principles

This policy evidences the commitment of senior management at CWC to achieve and maintain a high standard of information and cyber security throughout the Council.

The strategic approach to information and cyber security is based on:

- Consistency of approach with the implementation of key processes specified in the Information Governance Strategy.
- The application of recognised sources of security management good practice such as Cyber Essentials Plus which form the underlying basis of CWC key partner security standards, i.e. the Government (PSN compliance and the ten steps to reduce cyber risk), the NHS Data Security and Protection Toolkit (DPST), and most other public sector agencies and the implementation of physical, personnel, procedural and technical measures.

- A documented Information Security Management System (ISMS) which details CWC's information security management arrangements and the application of control measures in detail.
- Annual assessments of progress using CWC's Information Governance Strategy.
- The continuing availability of specialist information governance/security advice to support the implementation process for information and cyber security, and the other areas within the Information Governance Strategy.

And on the following principles:

- That information and cyber security is a vital area of concern that will receive the regular attention of senior management through the Senior Information Risk Owner, the Information Governance Board and Chief Cyber Officer.
- That information risk management will be at the heart of the improvement processes for information and cyber security.
- That all information users have an essential role to play in maintaining sound information and cyber security and they will be fully supported to enable them to achieve this.
- That successful implementation of information assurance across the Council is dependent on the full participation of all employees led by their designated Management Leadership Teams.

Key Elements of Information and Cyber Security Policy Management

This policy will be supported by procedures, standards, guidance, and training that aligned to recognised sources of security management good practice, such as the appropriate use of Council assets, Digital and IT Technical Standards and other Information Governance policies.

The main headings in the Information and Cyber Security Policy are:

- Risk Management
- Engagement and Training
- Asset Management including information handling
- Architecture and Configuration
- Vulnerability management
- Identity and Access management
- Data Security
- Logging and monitoring
- Incident Management
- Supply Chain Security

It is important that clear distinction is drawn between the responsibilities set out in this document below for all users, managers, Management Leadership Teams, and

Digital and IT services management.

Information and cyber security must not be seen as solely the responsibility of Digital and IT Services. The majority of information and cyber security breaches occur as the result of poor information handling by employees and consequently requires the attention of all users, their managers, and Management Leadership Teams in order to adequately protect CWC information.

Managers, and Leadership Teams are responsible for ensuring that their employees are aware of, and comply with, their responsibilities as set out under the headings of this policy.

Risk Management

All staff

- Communicate any information risks related to the Council's priorities and objectives to either managers, the Senior Information Risk Owner, Data Protection Officer, Information Governance specialists or Management Leadership Teams.
- Consider information risks and the technical and non-technical controls you can apply to manage those risks to ensure any adverse effect on the delivery of Council services is minimised.
- Consider information risks outside of your direct control related to supply chain security, third party services and cloud services.

Managers

- Identify and record key operational services and sensitive information on an information asset register identifying any risks and ensuring that assurances are put in place to mitigate such risks.
- Regularly review information risks to ensure that the ways you have decided to manage them remain effective and appropriate. In particular, revisit your risk assessments when something significant changes.

Engagement and Training

All Staff

- Ensure all mandatory data protection training is undertaken and successfully completed both at induction and in accordance with specified reminder dates.
- Understand what your job entails and identify and complete appropriate information and cyber security training to understand the risks involved.
- Undertake and complete any information and cyber security awareness training/campaigns as directed by the Council.

Managers

- Ensure employees undertake and successfully complete all appropriate information governance and cyber security training as part of the Professional Conversations process and maintain user awareness of information risks.
- Engage with employees to learn what potential barriers exist that may prevent them from following security procedures and work to remove those barriers.
- Understand and prioritise the information governance and cyber security knowledge and behaviours that employees in your service area need to ensure they receive appropriate training.

Asset Management, information handling and protective marking

All staff

- Take precautions to protect information both in transit and at rest in compliance with information governance training and guidance.
- Users must be able to identify potential information incidents and act appropriately when they occur.
- All emails and documents must be considered as to whether they should be protectively marked, in accordance with the sensitivity of their content, in line with this policy. The protective marking of a document provides the information user with the following:
  - The correct level of protection that the document should be given.
  - The procedures to be followed regarding the handling, transmission, storage, and disposal of the document.
  - The severity or impact of the loss or disclosure of the document.
- All information for internal and partner use will be protectively marked using the agreed markings detailed within this policy and must be used by all employees.
- Employees must assess all information for a protective marking. The protective markings to be used within the Council are:

Protective marking title	Description
RESTRICTED	Information to be restricted at a higher level of assurance than “PROTECT”, due to significant inconvenience, damage, harm or financial impact to the Council or individuals. This marking applies to the holding, storage and transmission of bulk customer or employee records and access will be restricted. There will be clear markings on the information as “RESTRICTED”.
PROTECT	Information where disclosure or unauthorised access would be inappropriate, inconvenient or cause harm

Protective marking title	Description
	or financial impact will be clearly marked as "PROTECT".
NOT PROTECTIVELY MARKED	Where neither of the above marking apply the information should be marked "NOT PROTECTIVELY MARKED" to make clear to the information user that the information has been assessed and not simply overlooked. For 'Not Protectively Marked' information a) anyone can potentially access the information internally or externally. b) It can be published on the web or in paper form but note that information may still be covered by copyright restrictions.
NO MARKING	Information produced for publication, or correspondence to the public should not be marked in anyway.
UNMARKED INFORMATION	Unmarked information will be unmarked for a variety of reasons, and this should be borne in mind by the information user. The possibilities are that: • Its originator has omitted to assess and mark the document. In this case the originator or the person with current responsibility for the document should be asked to assess and mark the document accordingly. Note that any change to the marking of a document must always be approved by the originator where possible. • The information pre-dates the adoption of the marking scheme by the Council or the organisation that it came from. If it is not feasible to ask the originator as above, then the information user should assess the document and mark it, accordingly, consulting their line manager if there is any uncertainty. • It is a publication or document / correspondence for the public. **Note:** The Government Security Classification policy has three levels of protective marking, Official; Secret and Top Secret. Only Official marking is likely to be routinely used in local government. Some documents may be marked Official-Sensitive. 'OFFICIAL-SENSITIVE' is not a classification. 'Sensitive' is a

Protective marking title	Description
	handling caveat for a small subset of information marked OFFICIAL that requires special handling. [*If documents from government departments marked Secret or Top Secret are received, please refer to Information Governance for guidance*.]

- The protective markings do not impose any specific restrictions on the supply of information under the Freedom of Information Act, the Data Protection Act, or the Environmental Information Regulations. However, they may indicate that all or some of the information may be subject to exemptions, for example personal information or commercially sensitive information.
- Some protective markings will need to be reviewed during the life of the information or document to ensure the marking is appropriate and still relevant.
- The destruction of information must be appropriate to its protective marking.
- All information must be stored and handled appropriate to its protective marking.

Managers

- Identify and understand what is the most important information, and technology, required to deliver the Council's objectives and services, assess the impact if that information or technology is compromised in some way and integrate this into your information asset register.
- Decommission any systems or information that are no longer used or that cannot be linked to a business need. Ensure that data is removed, and any corresponding accounts or credentials are disabled as part of the decommissioning process.
- Control and track IT equipment used off-site and return CWC assets at employment termination.

Architecture and Configuration

All staff

- Comply with instructions to restart your computer upon request to ensure software updates are successfully installed.

Managers

- Obtain and engage with the necessary expertise to design and maintain information systems that have the appropriate security controls built-in to protect privacy and mitigate the risks of cyber-attacks.

Vulnerability management, Logging and Monitoring

All Staff

- Report any unusual activity to the Digital and IT Service Desk.

Managers

- Test the ability to detect common cyber-attacks and/or incidents with exercises and incorporate any lessons learnt from both these exercises and actual incidents into monitoring solutions to help improve information system security.

Identity and Access management

All Staff

- Employees, agency staff, contractors and third parties will be given individual accounts and access to information will be subject to management processes that limit user privileges.

Managers

- User access will be suitably administered to ensure that the type of account granted to employees is such that it allows them to perform their day-to-day user activities and prevents access to any sensitive information and key operational services not required for the purpose of undertaking their duties.
- Ensure members of staff, contractors and third-party access to information systems does not exceed the needs of the role on a 'need to know' basis; that their use of IT is appropriate; and that starter, leaver and amendment changes are properly processed and authorized on a timely basis.
- Ensure that confidentiality agreements are in place for both Council and non-Council employees (including for example: contractors, students volunteers, partner agency workers) where sensitive personal or confidential information may be accessed.

Data Security

All staff

- All removable media must be scanned for malware before importing on to the corporate network.
- Encrypted removable media should be used at all times and always when transferring sensitive data. This is to prevent the potential loss of any sensitive data.
- Report any unusual activity to the Digital and IT Service Desk.

Managers

- Ensure the use of any removable media is kept to a minimum, encrypted and that any types of information held on such devices can be transferred /

imported into the Council's systems to prevent the actual or potential loss of any sensitive data.

- Report any unusual activity to the Digital and IT Service Desk and ensure compliance with the
- Council's Information Governance and associated policies is maintained.

Incident Management

All staff

- Understand your role and responsibilities in incident reporting, response plans, disaster recovery and business continuity plans that impact sensitive information or key services.

Managers

- Establish and maintain a defined, planned, and tested response to cyber security incidents that could impact sensitive information or key operational services.
- Establish and maintain well defined and tested processes to ensure the continuity of key operational services in the event of failure or compromise.
- Practice and test response plans to ensure employees know how to respond during an incident. Use of the National Cyber Security Centre's (NCSC) 'Exercise in a Box (ncsc.gov.uk)' to help test and practice responding to different types of cyber-attack.
- Update response plans after every incident or test to reflect any learning that would help prevent any future incidents and insights into how to improve future plans.

Supply Chain Security

All staff

- As part of procurement processes verify what security certifications suppliers hold e.g., Cyber Essentials; Cyber Essentials Plus; ISO27001- Information Security Management as these indicate a proactive approach to cyber security. Without any of these certifications more information in respect of firewalls, secure configuration, user access control, malware protection and patch management will be required.
- In respect of the provision of online services attention should be paid to the most common web application security issues. Review using the Open Web Application Security Project (OWASP) Top 10

Managers

- Maintain a current list of suppliers, and partners, identifying those who handle sensitive information, or are involved with key operational services and ensure you understand the security responsibilities of all parties.

- Provide assistance, when necessary, where security incidents in the supply chain have the potential to affect the delivery of services.
- Include important suppliers/partners in incident response planning and exercises where appropriate.

Roles and Monitoring

Digital and IT Service are responsible for documenting and maintaining the wide range of technical standards required to enable the Information and Cyber Security policy, in line with Security Best Practice and Government Guidelines. These include standards for:

- Architecture and configuration
- Vulnerability management
- Identity and access management
- Data security
- Logging and monitoring
- Data Backup and restoration plans

The Chief Cyber Officer will:

- Provide subject matter expertise and advice to the Information Governance Board on a broad range of cyber risk and security activities including; the collection of Digital and IT tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and the information assets of the Council and users;
- Ensure that information from Government and across the IT industry regarding the identification of new threats and vulnerabilities is reliable, kept up to date and responded to appropriately;
- Oversee arrangements to ensure that IT network security risks in both on-going and planned operations, system developments and projects are properly considered;
- Provide expertise in support of the execution of actions designed to mitigate risks, strengthen defence, and reduce vulnerabilities in the following key areas described in this policy.

Please find a description of other relevant roles and responsibilities available on the Information Governance pages of the Councils public website here; What is Information Governance? | City Of Wolverhampton Council

This policy will be approved and monitored by the Councils Information Governance Board. It will be reviewed every 2 years or sooner if legislative changes require.

Training and dissemination

The Council will ensure that everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice.

All relevant employees are mandated to complete the Councils protecting information training upon induction and are required to update their training on this subject matter on a regular basis.

Specialised training will be made available to employees where their role requires them to handle higher volumes of personal data or data that is more sensitive in nature.

Links to other Policies

This Policy forms part of the Information Governance Framework and should be read in conjunction with the other related policies within the framework which are outlined below. They are available on the Information Governance pages of the Councils public website here: What is Information Governance? | City Of Wolverhampton Council

- IG00 Strategy
- AI00 Access to Council Information
- DP00 Data Protection Policy
- RM00 Records Management Policy
- Information Governance Definitions, Roles and Responsibilities