CITY OF
WOLVERHAMPTON
COUNCIL

# Information and Cyber Security Policy

**Change History**

| Version | Date | Description | Author |
|---|---|---|---|
| 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 | 12/04/13 | Revised following IGB consultation | Anna Moore |
| 0.5 | 23/04/15 | Revised to take account of cyber risks | Martin Eades |
| 0.5 | 16/08/16 | Revisions approved by SEB | Martin Eades |
| 0.6 | 23/05/18 | Revised to take account of GDPR | Martin Eades |

## Contents

1. Introduction 4

2. Purpose 4

3. Scope 4

4. Legal and Regulatory Regulations 5

5. Policy 5

5.1 Strategic Approach and Principles 5

5.2 Approach to Information Risk Management 6

5.3 Key Elements of Information Security Management 6

5.4 Awareness of Information Security Policies and Procedures 6

5.5 Roles and Responsibilities 6

5.5.1 All Users 7

5.5.2 Managers 8

5.5.3 ICT Services 10

5.5.4 Information Governance / Security Roles 10

5.5.5 Senior Information Risk Owner (SIRO) 11

5.5.6 Chief Cyber Officer 11

5.5.7 Information Asset Owners 12

5.5.8 Information Governance Board (IGB) 12

5.6 Compliance 13

5.7 Review 13

## 1. Introduction

City of Wolverhampton Council (CWC) is making increasing use of the range of information, including service user information, held by the Council and other public sector organisations in order to ensure the continued delivery of services. In addition, the Council is making increasing use of ICT 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 public confidence and ensure that the Council complies with relevant statutory legislation, it is vital that CWC maintains the highest standards of information security and has policies to support and maintain these standards.

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

## 2. Purpose

The objective of this information and cyber security policy and its supporting policies is to ensure the highest standards are maintained across the Council at all times so that:

a) The public and all users of the Council's information are confident of the confidentiality, integrity and availability of the information used and produced.

b) Business damage and interruption caused by cyber security incidents are minimised.

c) All legislative and regulatory requirements are met.

d) 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. This policy will be supported by more detailed policies covering more specific aspects of information and cyber security.

## 3. Scope

This policy applies to all information held or owned by CWC, any ICT equipment and infrastructure used, and the physical environment in which the information and/or supporting ICT 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).

The policy applies automatically to all CWC Councillors, committees, departments, partners, employees, contractual third parties and agents of the Council.

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.

## 4. Legal and Regulatory Obligations

The Council's statutory obligation to have sound information and cyber security arrangements in place originates in the General Data Protection Regulation (EU) 2016/679, 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 ICT 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; meet Payment Card Industry Data Security Standards (PCI DSS) or receive or share information with partner agencies under information sharing arrangements.

## 5. Policy

### 5.1 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:

a) Consistency of approach with the implementation of key processes specified in the Information Governance Framework.

b) The application of recognized sources of security management good practice such as the ISO/IEC 27000 family of information security management systems standards 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 (the Information Governance Toolkit), and most other public sector agencies and the implementation of physical, personnel, procedural and technical measures.

c) A documented Information Security Management System (ISMS) which details CWC's information security management arrangements and the application of control measures in detail.

d) Six monthly assessments of progress using CWC's Information Governance Framework.

d) 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 Framework.

And on the following principles:

a) 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.

b) That information risk management will be at the heart of the improvement processes for information and cyber security.

c) 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.

d) That successful implementation of information assurance across the Council is dependent on the full participation by Directorates led by their designated Information Asset Owners (IAOs).

### 5.2 Approach to Information Risk Management

The Information Risk Management Policy sets out CWC's approach to information risk management and the key roles and responsibilities under that policy.

### 5.3 Key Elements of Information and Cyber Security Policy Management

This policy will be supported by more detailed policies, procedures, standards, guidance and training that align to recognised sources of security management good practice, such as appropriate use of council assets, ICT Technical Standards and other Information Governance policies.

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

i. Home and Mobile Working
ii. User Education and Awareness
iii. Incident Management
iv. Information Risk Management Regime
v. Managing User Privileges
vi. Removable Media Controls
vii. Monitoring
viii. Secure Configuration
ix. Malware Protection
x. Network Security

### 5.4 Awareness of Information and Cyber Security Policy and Procedures

Information and Cyber Security Policy and procedures will underpin mandatory corporate information governance training and periodic refresher training for all users of CWC information systems The training will be supported by further detailed information available on the CWC intranet/SharePoint. Users who do not complete the mandatory information governance training - will either not be granted access to CWC information systems or have their access suspended.

### 5.5 Roles and Responsibilities

It is important that clear distinction is drawn between the responsibilities set out in this document below for all users, managers, information asset owners and ICT services management. Information and cyber security must not be seen as solely the responsibility of

ICT 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 information asset owners in order to adequately protect CWC information.

### 5.5.1 All Users

There are a few key issues that are central to good security and all CWC information users must be aware of and comply with the relevant Council policies. These are listed in summary here, but users must refer to the specific policies and guidance listed in the footnotes.

**i. Home and Mobile Working**

ICT access security is centred on each authorised user having a unique user id and a strong password that is kept secret and known only to them[1]. User id and passwords must not be shared or used by anyone other than the authorized user.

Take precautions to protect information both in transit and at rest in compliance with information governance training and guidance.

Undertake mandatory and recommended information governance training to understand the risks involved with Home and Mobile Working.

**ii. User Education and Awareness**

- Data Protection
  - ➢ The Data Protection Act is the key legislation affecting the use of personal data. Illegal disclosure of personal information can lead to the Council or the individual responsible being heavily penalised so all those handling personal information must understand and comply with the Act[2].
- Information Handing
  - ➢ Detailed Information security and handling procedures are designed to protect the Council from identified business impacts in the event of the loss of confidentiality, integrity or availability of information[3].
- Work Environment
  - ➢ Clear desk implementation, secure handling of information, and secure location of workstation screens – including ensuring use of screen locking[4]

Undertake mandatory and recommended information governance training and be aware of the Council’s Information Governance Framework and associated policies.

[1] Policy on Personal Use of Council Equipment, and Access to Social Media

[2] Data Protection Policy

[3] Information Protective Marking and Handling Policy

[4] Clear Desk Policy

### iii. Incident Management

Users must be able to identify potential information incidents and act appropriately when they occur by following procedures set out in the Information Incident Policy.

### iv. Information Risk Management Regime

Communicate any information risks to either managers, the Senior Information Risk Owner, Information Asset Owners or Information Governance specialists.

### v. Managing User Privileges

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.

### vi. Removable Media Controls

All removable media must be scanned for malware before importing on to the corporate network.

Encrypted removable media should be used wherever possible and always when transferring sensitive data. This is to prevent the potential loss of any sensitive data.

Undertake mandatory and recommended information governance training to understand the risks involved.

### vii. Monitoring

Report any unusual activity to the ICT Service Desk.

### viii. Secure Configuration

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

### ix. Malware Protection

Report any unusual activity to the ICT Service Desk.

### x. Network Security

Report any unusual activity to the ICT Service Desk.

## 5.5.2 Managers

Managers are responsible for ensuring that they and their employees:

- Are aware of, and comply with, their responsibilities under the headings detailed above in 5.5.1.

- Undertake all identified mandatory information governance training.

In addition, they have responsibilities for

i. **Home and Mobile Working**

Assess the risks to all types of home and mobile working and ensure employees have received suitable training and guidance

ii. **User Education and Awareness**

Ensure employees undertake and successfully complete all appropriate information governance training as part of the employee appraisals and maintain user awareness of information risks.

iii. **Incident Management**

Ensure plans are in place to recover from any disasters and maintain business continuity

Report and respond to any actual or potential information incidents in accordance with the Council's Information Incident Policy.

iv. **Information Risk Management Regime**

Identify and ensure any information risks are recorded on the risk register and ensure that assurances are put in place to mitigate such risks.

Control and track ICT equipment used off site, and return CWC
assets at employment termination[5].

v. **Managing User Privileges**

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 not required for the purpose of undertaking their duties.

Ensuring 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 ICT is appropriate; and that starter, leaver and amendment changes are properly processed and authorised[6].

- Confidentiality and Third-Party Agreements

  Ensuring that confidentiality agreements are in place for non-Council staff (including for example: contractors, students volunteers, partner agency workers) where personal or confidential information may be accessed.

[5] ICT Infrastructure Security Policy, ICT Portal – Governance

[6] Human Resources Behaviour Standards and Code of Conduct

### vi. Removable Media Controls

Ensure the use of any removable media is kept to a minimum 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.

### vii. Monitoring

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

### viii. Secure Configuration

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

### ix. Malware Protection

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

### x. Network Security

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

### 5.5.3 ICT Services

ICT 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 the following:

- Network Security
- Secure Configuration
- Malware Prevention
- Removable Media Controls
- Monitoring
- Access /Permission controls

### 5.5.4 Information Governance / Security Specialist Roles

Information governance and security specialist roles within CWC are responsible for supporting the Senior Information Risk Owner and the Information Asset Owners in the planning and implementation of processes according to the Information Governance Framework and the Information Security Standards.

### 5.5.5 Senior Information Risk Owner (SIRO)

The SIRO will:

- Take overall ownership of the Council's Information Governance Framework acting as champion for information governance;

- Provide advice and reports to the Managing Director in respect of information incidents and risks, including the content of the Council's Annual Governance Statement in regard to information risk;

- Provide an annual report to the Managing Director on their work;

- Understand how the strategic goals of the Council may be impacted by information governance risks, and how these risks may be managed including the adequacy of levels of independent scrutiny;

- Provide a focus for the management of information governance at Board level; and

- Owns the management of information governance and risk assessment processes within the Council including the provision of advice on the effectiveness of information risk management across the Council[7].

### 5.5.6 Chief Cyber Officer

The Chief Cyber Officer will[8]:

- 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 ICT 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;

[7] See Information Governance Board – changes to terms of reference and definitions, roles and responsibilities Cabinet (Performance Management) Panel 15:09:2014

[8] See Information Governance Board – changes to membership and roles Cabinet (Performance Management) Panel 23:02:2015

- Provide expertise in support of the execution of actions designed to mitigate risks, strengthen defence and reduce vulnerabilities in the following key areas:
  - Home and Mobile Working
  - User Education and Awareness
  - Incident Management
  - Information Risk Management
  - Managing User Privileges
  - Removable Media Controls
  - Monitoring
  - Secure Configuration
  - Malware Protection
  - Network Security

### 5.5.7 Information Asset Owners

Information Asset Owners[9] are responsible for:

- Ensuring that information risk assessments or reviews are performed at quarterly on all information assets where they have been assigned ownership and in accordance with the Information Risk Assessment Guidelines.

- Submitting the risk assessment results and associated mitigation plans to the Senior Information Asset Owner (SIRO) for review.

- Ensuring the compilation and maintenance of the Information Asset Register entries for all their owned assets.

- Ensuring that information is classified according to the Council's Information Protective Marking Scheme and its potential business impact.

- Ensuring that services implement all information governance policies and their supporting processes as set out in the Information Governance Policy.

### 5.5.8 Information Governance Board (IGB)[7]

The purpose of this Board is to support and drive the development of effective corporate strategies to ensure City of Wolverhampton Council puts in place appropriate information risk management activities and complies with best practice mechanisms, legislative requirements and standards in respect of the confidentiality, integrity, availability and security of information.

[9] Information Risk Management Policy

## 5.6 Compliance

Compliance with this policy and related standards and guidance will be monitored as part of the work of the Information Governance Board and supported by the work of Audit Services.

As part of the monitoring and evaluation, an action plan for improvements in information security practices will be formulated as required by the Information Governance Board.

## 5.7 Review

A review of this policy will take place at least annually to take account of any new or changed legislation, regulations or business practices.