Information Security Policy

Version: 2.1
Date Issue: May 2018
Review date: April 2020
Reference: WCCC-1162-15
Team: Cyber Security
Protective Marking: Internal

Warwickshire County Council

Working for Warwickshire

Document Control

Title:	Information Security Policy
Issued by:	Information Security
Date:	09/05/2018
Author	Morgon Evans
Version:	2.1
Status:	Released

Revision History

REVISION	DATE	REVISION STATUS
0.1	23/09/2013	Draft
1.0	27/09/2013	Released
1.1	16/02/2017	Draft
2.0	25/05/2017	Released
2.1	09/05/2018	Released

Document Review

REVIEWER	**POSITION**	**DATE**
Charles Hunter	Security Policy and Awareness Officer	23/09/2013
Les Harlock	Information Security Manager	23/09/2013
	Senior Information Risk Officer	27/09/2013
Charles Hunter	Security Policy, Guidance and Awareness Officer	16/02/2017
Morgon Evans	Cyber Security Manager	16/02/2017
Graham Dunnings	Cyber Security Consultant	09/05/2018
Morgon Evans	Cyber Security Manager	09/05/2018
IGSG	Information Governance Steering Group	18/05/2017

Scope

This policy applies to:

- All Councillors and staff; "Staff" includes all employees, Councillors, secondees, volunteers, work experience and any other individuals working for the Council on a contractual basis.

The policies and security requirements in this document refer to and gain authority from the WCC Information Security Policy statement as authorised and issued by the WCC Chief Executive and can be enforced accordingly.

Information, and the systems which support it, are vital important Council assets. Their availability, integrity, security and confidentiality are essential to maintain service levels, legal compliance and the image and perception of the Council. Threats to the security of information/data are becoming more widespread, ambitious and increasingly more sophisticated and we must maintain a policy to reflect this ever-changing environment.

The purpose of this Policy is to inform staff and protect WCC from security issues that might have an adverse impact on our organisation.

Security issues can include:

- **Confidentiality** (the wrong people obtaining information),
- **Integrity** (information being altered without permission, whether deliberate or accidental) and
- **Availability** (information not being available when it is required and needed).

Information Security Policy Statement

Warwickshire County Council's activities are critically dependent on information and information systems. Consequently, the Council has a continual commitment to protect Council and stakeholder information.

To this end, the application of Information Security across Warwickshire County Council is founded upon the following guiding principles:

- Information is a critical asset. All storage and transmission of information processed or controlled by Warwickshire County Council must only be carried out for the lawful purposes for which it is held.
- Information will be classified and protected in a manner commensurate with its sensitivity, value, and criticality.
- Information will be protected from loss of confidentiality, integrity and availability.
- Warwickshire County Council information should only be provided on a need to know basis and disclosed only to those people who have a legitimate need for that information.
- Information security requirements will be identified by assessment of risks to determine the balance of investment in information security against the risk to Warwickshire County Council and its stakeholders.
- A process of continual review and improvement will be implemented.
- Users, resources or processes that store, transmit or process information will have no more privileges than necessary to be able to fulfil their function.
- All relevant regulatory and legislative Information Security requirements will be met.
- All incidents and losses, regarding Information Security, actual or suspected, must be reported to Information Security.
- All systems must be reviewed, prior to implementation, and undergo a rigorous security assessment as part of that process.
- All Warwickshire County Council managers are responsible for the implementation of Information Security Policies within their areas.
- Disregard for these Security Policies may be regarded as misconduct to which the County Council's Dismissal and Disciplinary Procedure applies and a serious breach of any policy may be treated as gross misconduct and may lead to dismissal.
- All staff are responsible for upholding this policy, under the guidance and with the assistance of the Information Security Manager.
- Warwickshire County Council will provide appropriate security awareness training to all staff and provide specific security training where required, thereby developing and supporting a security and risk aware culture throughout the County Council.

Contents

1. Passwords and Authentication

The purpose of this section is to establish standards for the creation, protection and use of passwords across and within WCC.

They must ALWAYS be used in conjunction with a Unique User ID.

All system passwords are to be treated as 'sensitive' information.

WCC staff must not:

- Share system passwords with anyone, including peers, assistants or superiors.
- Discuss or talk about a password in front of others.
- Hint at the format of a password (e.g., "my family name").
- Reveal a password on any questionnaires.
- Share a password with family members.
- Reveal a system password to co-workers providing holiday or absence cover.
- Write passwords down.
- Store unencrypted passwords in a file on ANY computer system.
- Use the "Remember Password" feature of any applications.

WCC staff must immediately change a password if they suspect that it has been compromised, following which they must immediately report the incident to Information Security.

Password length must be a minimum of 8 characters or a minimum of 15 for system administration passwords.

Where technically possible, passwords should expire no later than 90 days

Password and Authentication Policy

2. Anti-Malware

The purpose of this section is to establish requirements, which must be met by all devices within WCC's computing infrastructure, to protect the confidentiality, integrity and availability of WCC software and information assets from the effects of malware.

- Unless undertaken by or following instruction from ICT support staff, WCC staff must not disable anti-malware software running on, or prevent updates being applied to, devices within the WCC computing infrastructure.
- The intentional introduction of viruses to WCC's computing infrastructure is strictly prohibited.
- Only software that has been authorised by WCC can be installed upon WCC systems.
- Each WCC member of staff is responsible for immediately reporting any abnormal behaviour of WCC computing systems to the ICT service desk.
- Prior to any encryption, all files must be scanned for and cleaned of viruses before being sent to any third party.
- All members of staff are responsible for ensuring that appropriate and effective anti-virus detection software is installed and running, where technically possible, on all personal devices that are used to access WCC Corporate information.

3. Access Control

- Access to specific resources is only to be granted to authorised personnel who have a legitimate need to use those resources.
- Users of WCC information will have no more privileges than necessary to be able to fulfil their role. Additionally, "segregation of duties" must also be enforced so no one individual can carry out a critical task alone that could prove to be detrimental to the Council or its stakeholders.
- All requests for access to WCC computer systems must be via a Cyber Security approved systems access request process.
- WCC reserves the right to revoke access to any or all of its computer systems at any time.
- Regarding inappropriate access:
    - Users of WCC systems must immediately report to the ICT Service

Desk if they have an inappropriate access level to a WCC system.

- If they have observed that another user has an inappropriate access level to a WCC System, then they are required to raise this with their Line Manager unless they feel they are not in a position to. In that case, they must contact a Head of Service, or Director, to raise this potential security incident.

- Accounts are to be created so that the identity of all users can be established and activity audited at any time during their computer usage.
- Users must not circumvent the permissions granted to their accounts in order to gain unauthorised access to information resources.
- Users must not allow anyone else to use their account, or use their computers while logged in with their account.
- Computer screens should be 'locked' or the user logged out before leaving any workstation or device unattended.
- Users should not leave workstations or devices in 'sleep mode' for convenience

4. Clear Desk and Clear Screen

WCC has adopted both a Clear Desk and Clear Screen Policy to reduce the risk of unauthorised access, loss of, and damage to information during and outside normal working hours or when work areas and computers are unattended.

The purpose of this section is to establish WCC's requirements to ensure that information is not disclosed by being made available in any form to unauthorised individuals.

- It should be assumed at all times that individuals, other than WCC employees, have access to office areas. Consequently, no information should be left on a desk surface overnight or when the desk is unoccupied.
- Removable media and easily portable devices, such as laptop computers or iPads, that have not been physically secured, must not be left unattended on desks.
- Where practically possible, paper, computer media and portable computing equipment should be stored in suitable locked safes, cabinets or other forms of security furniture when not in use.
- Where lockable safes, filing cabinets, drawers, cupboards etc are not available, office / room doors must be locked if left unattended.
- At the end of each working day all sensitive information must be stored in locked furniture.
- All information, when printed, faxed or photocopied, is to be cleared from printers, faxes and photocopiers immediately and, when no longer required, destroyed in a secure and reliable manner using approved methods.
- Reception areas, and other areas of high levels of foot traffic, should be kept as clear as possible at all times; in particular Council information classified as 'WCC Confidential' or 'personal' should not be held on a reception desk within reach or sight of visitors.
- Any visit, appointment or message books should be stored in a locked area when not in use.
- When vacating meeting rooms or shared areas the area must be checked to ensure that no information, regardless of format, has been left behind. All whiteboards must be cleaned of information, and used flipchart pages must be removed and disposed of securely.
- Computer screens should be 'locked' or the user logged out before leaving any workstation unattended, even for a brief period.
- Users should not leave workstations or devices in 'sleep mode' for convenience.

Link to Accommodation Standards

5. Mobile Computing

Mobile computing within Warwickshire County Council (WCC) has enabled flexible working practices intended to improve work/life balance. However, mobile computing also creates specific information security issues as the loss of or theft of mobile computing devices could potentially lead to:

- ***Risk of disclosure of information***
- ***Risk of loss of information***
- ***Risk of unauthorised access to WCC network or information***
- ***Risks of loss of valuable equipment***

The purpose of this section is to ensure that information assets and information processing facilities, used to access WCC information, are adequately protected with logical, physical and environmental controls when being used by mobile employees.

Mobile Computing Equipment supplied by the Council is for the sole use of authorised personnel and access to information stored on these devices is not to be shared with unauthorised persons for any purpose whatsoever and is the responsibility of the employee to ensure that information is not shared or disclosed to unauthorised persons.

Staff will be made aware of their responsibility to:

- Protect any mobile computing equipment that they have been supplied with by WCC.
- Ensure that any mobile device for which they are responsible is securely locked away when left on WCC premises overnight.
- Promptly report to the ICT Service Desk, and their immediate Line Manager, any known or suspected security breach or loss of the device.
- Avoid the risk of being overlooked or overheard by unauthorised persons when using mobile computing or phone facilities in public places, meeting rooms and other areas outside of WCC premises.

WCC information classified as 'WCC Confidential' or 'personal' must not be discussed or otherwise exposed in public, where unauthorised people might discover it. For clarification, please refer to the WCC Information Risk and Protective Marking standard

Mobile Workers are responsible for ensuring that information held locally is backed

up regularly to the WCC network, based on the importance of their data. If backup via the WCC network is not available or feasible, mobile workers should create a local backup of their data on an encrypted device.

Further detail can be found in the **Mobile Computing Policy (under review)**.

6. Removable Media Devices

The purpose of this section is to establish control requirements for the use of removable media devices within and across WCC.

- Only Approved devices will be issued to and used by WCC Staff for the storage of WCC Data, regardless of classification.
- The Approved device is for the short term storage/transfer of WCC data, not to have the data written to the device and never removed.
- Staff MUST NOT use an unapproved device for the storage of ANY WCC data.
- Passwords applied to Approved Encrypted Devices MUST adhere to the Password and Authentication Policy
- Data found to be residing on Unapproved USB storage devices MUST be immediately removed.
- Staff will surrender the device to WCC ICT Services on demand or when leaving WCC and ICT Services will be responsible for its destruction. Staff that leave WCC and retain WCC data on any removable device, approved or otherwise, may be subject to section 55 of the Data Protection Act in regard to Unlawful Obtaining of Data. This is a criminal offence.

7. Encryption

Encryption must be utilised for the following areas:

- All WCC information classified as 'WCC Confidential' or 'personal' must be encrypted for transmission across the Internet.
- All WCC information classified as 'WCC Confidential' or 'personal' that is recorded on backup computer media and stored outside WCC offices must be encrypted prior to leaving WCC premises.
- Where encryption is used to protect 'WCC Confidential' or 'personal' data resident on computer storage media, the encryption keys and passwords used in the encryption process must not be stored anywhere on or with this storage media in unencrypted form.

Only encryption technologies, algorithms and products that have been approved by WCC Information Security may be used.

8. Protective Monitoring of WCC Information Systems

The purpose of this section is to establish control requirements for the monitoring and logging of information security related events relating to the use of WCC's information and information systems.

The use of WCC's data communications infrastructure, services, systems and applications may be monitored by authorised personnel as permitted by UK legislation, which allows the monitoring of systems and network traffic without consent for legitimate purposes such as:

- Recording evidence of activity
- Policing regulatory compliance
- Detecting crime or unauthorised use
- Safeguarding the integrity of WCC's information and information systems

Authorised WCC personnel may monitor and analyse network services, systems, data (including file systems), applications and data communications facilities pertaining to WCC's business activities.

WCC staff are prohibited from engaging in monitoring activities or monitoring outside of their areas of responsibility without written authorisation from any of the following: Senior Management, HR, Legal Services and the Cyber Security team.

Network Security Policy

9. Security Incident Management

The purpose of this section is to ensure that WCC can respond to Security Incidents effectively and in a timely manner and that staff know, and understand, their roles and responsibilities when dealing with, and notifying us of, an Information Security Incident.

- It is the responsibility of each member of staff to report any suspicion or details about Information/Cyber Security Incidents to WCC's Cyber Security team by raising a call with the ICT Service Desk as soon as possible to help us deal with the incident swiftly by directing to the correct resource.
- WCC staff must never attempt to interfere with, prevent, obstruct, or dissuade an employee, in their efforts to report an Information Security problem or

violation, or retaliate against an individual for reporting or investigating

- Information about a security incident must only be supplied to the press or other news media with authorisation of a Head of Service and Corporate Communications.
- Unless compelled by local or UK law, or authorised by WCC Legal Services, staff must not report information security incidents to individuals or organisations external to WCC.
- All staff must be aware of and have access to a current documented procedure that clearly specifies how Information Security Incidents will be handled; all security incidents are dealt with by the Incident Group.
- Users of WCC information systems must immediately report to the ICT Service Desk, any unusual and suspicious activity such as unusual requests for information coming from any internal or external party, and abnormal system behaviour.
- WCC staff must immediately report to their manager any damage to or loss of WCC computer hardware (including portable devices), software, or information (electronic or paper) that has been entrusted to their care.
- All information security incidents must be handled with the involvement and cooperation of the Cyber Security Manager.
- Any member of staff who reports a security problem, vulnerability, or an unethical condition within WCC will be protected and their identity held in strict confidence, in line with WCC's Whistleblowing Policy.
- All investigations, where an individual is identified as a possible cause, must be kept strictly confidential to preserve the reputation of the suspected party as charges may be formalised and/or disciplinary action taken.

10. BYOD

BYOD stands for Bring Your Own Device. The purpose of this section is to help users understand their responsibilities when using their own devices with the WCC infrastructure.

- Do not store any WCC information in any other location other than the Google Services you are authorised to sign into and use
- When using WCC Google services, you must sign in and sign out, when finished. Under no circumstances are you to use any 'remember/save password' functionality that may be offered to you.
- If using your own device, to access WCC resources/information, you must ensure your device is regularly updated to the latest version, including all other apps and programs **BYOD Policy (under review)**

11. Starters and Leavers Data Access

With access now available to a wide array of systems, it is vital to have a correct policy for managing the flow of employees' access from the moment they join to when they leave.

HR have a process in place to deal with this and it must be followed in the event of a starter, leaver or anyone transferring internally:

Induction Process

Leavers Process

12. Secure Disposal Policy

All devices, data and information have a secure mechanism for disposal; here is the procedure from Information/Records Management that must be followed:

Confidential information disposal procedure

13. Acceptable Use Policy

The Acceptable Usage Policy covers the security and use of all WCC's information and IT equipment. It also includes the use of email, internet, voice and mobile IT equipment.

Acceptable Use Policy

14. Information Transfer Policy

This policy will help all employees understand their responsibilities when transferring information from WCC to any external third party.

Information Transfer Policy

Third Party Access Policy (under review)

This policy is designed to assist all staff understand their responsibilities when dealing with

any 3rd Party (including external vendors and supplier) that require any access to the WCC network.

Firewall Management Policy (under review)

This policy will detail all requirements for all employees who have responsibilities for, or dealings with, the WCC Firewall infrastructure.

Physical and Environment Policy (under review)

Whilst this is a Facilities policy, it also details all security requirements relevant to the physical environment at WCC.