Warwickshire
County Council

Information Security Policy

Document Control

Title:	Information Security Policy
Issued by:	Solutions Architecture
Date:	31/03/2025
Policy Owner:	Risk and Compliance Officer
Version:	3.0
Status:	Released
Protective Marking:	Internal

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
2.2	04/02/2020	Released
3.0	31/03/2025	Released

Document Review

REVIEWER	POSITION	DATE
Charles Hunter	Security Policy and Awareness Officer	23/09/2013
Les Harlock	Information Security Manager	23/09/2013
Tonino Ciuffini	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	16/02/2017
Morgon Evans	Cyber Security Manager	02/05/2017
Tricia Morrison	Senior Information Risk Officer/IGSG	18/05/2017
Graham Dunnings	Cyber Security Consultant	09/05/2018
Morgon Evans	Cyber Security Manager	09/05/2018
Tricia Morrison	Senior Information Risk Officer/IGSG	19/07/2018
Michael Parker	Senior Information Security Officer	20/01/2020
Daniel Hone	Production and Communications Services Manager	20/01/2020
IGSG	IGSG	04/02/2020
Tim Molloy	IT Risk and Compliance Officer	25/02/2025

Introduction

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.

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. Please consult the WCC **Information Risk and Protective Marking Standard** for more detail.
- 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 or losses, suspected or otherwise, involving WCC assets or data must be reported as per the WCC **Data breach, security incident reporting procedure**
- All systems must be reviewed, prior to implementation, and undergo a rigorous security assessment as part of that process at an early stage of the procurement 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 Risk and Compliance Officer.
- 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.

Scope

This policy applies to all Staff; “Staff” includes all employees, Councillors, secondees, volunteers, work experience and all contractors.

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 vitally important Council assets. Their availability, integrity, security, and confidentiality are essential to maintain service levels, legal compliance, and the reputation of the Council. Threats to the security of information/data and systems 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).

What happens if it is not possible to follow the policy (or it becomes known that it has not been followed)?

The policy will work well in most cases, but in exceptional situations where it can't be followed, an email should be sent to ictrisk@warwickshire.gov.uk. The email should detail the area of the policy that there is a problem with the business reason, and any relevant context and data. Our Solution Architecture Team will then work with you on the best way forward.

The team will carefully review the detail you send, and a final decision will be taken by the Risk and Compliance Officer following consultation where required. Where the exception is agreed, the Risk and Compliance Decision Log (RCDL) will be updated by the Risk and Compliance Officer.

We are all human and mistakes happen, so where the policy has not been followed and the above risk assessment and review hasn't been completed (and the instance is not recorded on the RCDL), the ICT Service Desk MUST be notified as soon as possible so that we can best manage the situation. The context behind some situations will require disciplinary action to be taken. In particularly serious circumstances this could lead to dismissal and, where a law has (or has believed to have) been broken or breached, it will be necessary to involve the relevant law enforcement authorities. We hope that we never need to get to the point of disciplinary action, which is why following this policy (or working with ICT Risk via a risk assessment) is the best way forward.

Where you believe a data breach has, or may have, occurred the reporting procedure can be found on the Warwickshire SharePoint site under:

Data breach, security incident reporting

1. Passwords and Authentication

The Password and Authentication Policy will instruct Staff to the current rules that MUST be met to use, implement, or manage passwords and PINs within the scope of any WCC ICT system. The policy will allow Staff to follow any best practices for password and PIN management to assist in protecting WCC assets from unauthorised access.

All system passwords are to be treated as ‘sensitive’ information.

WCC staff must **NOT**:

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

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

Please consult WCC’s Password Policy for Individuals for more details

2. Anti-Malware

The word ‘malware’ is used to group many types of malicious software, including, but not limited to, viruses, ransomware, worms, trojans, macros and rootkits, or any other type of software which attempts to damage ICT services in a malicious way.

Malware poses a serious threat to all WCC ICT services and the impact from a successful attack could cause loss of confidentiality, integrity and availability of ICT services and/or WCC information assets.

The Anti-Malware Policy sets out where Anti-Malware controls are to be implemented and how they must be used. The policy also aims to set out User responsibilities to help protect against malicious software infection.

Please consult the WCC Anti-Malware Policy for more details

Vulnerability Management

The timely and secure management of vulnerabilities is critical. WCC uses a plethora of software to deliver its services. It is important to ensure operating systems, apps and software is updated regularly to patch any vulnerabilities.

WCC are bound by several sets of rules such as PCI, PSN Code of Connection and NCSC guidance to ensure patches are kept up to date. WCC need to be able to demonstrate that timely patch management is being actively undertaken.

Please consult the WCC Vulnerability Management Policy for more details.

3. Access Control

Access control determines who can access what data, based on business requirements and legal responsibilities. Users only require access to certain data assets in the course of their work at WCC and it is the responsibility of the Information Asset Owner (IAO) to ensure that job roles are given the correct access to the data assets within their control. Note: If you require access to data or a system then requests should be sent via an authorised method as agreed with your Line Manager. Direct requests to IAO’s are not normally expected.

The Access Control Policy will instruct staff to the current rules that MUST be met to use, implement, or manage access control within the scope of any WCC managed device or system/service. The policy will allow staff to follow any best practices for access control and access management to assist in protecting WCC.

Please consult WCC’s **Access Control Policy f**or more details.

4. Secure Disposal

The security of information is as important when disposing of it as it is while it is in use. WCC remains responsible for information and faces action from the Information Commissioner if information, which should have been confidentially disposed of results in being lost and/or is in the public domain.

The Secure Disposal Policy details the current WCC rules regarding secure disposal to help ensure correct and secure destruction.

Please be aware there may be instances when data retention requirements must be clarified prior to destruction. If staff have any questions, suggestions or would like advice in regard to requirements for data retention and disposal then please contact Information Management.

Please consult WCC's **Secure Disposal Policy** for more detail.

5. 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 always assumed 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, Surface Pro computers or iPads, which have not been physically secured, should not be left unattended on desks, especially in public areas.
- Computer screens should be 'locked' or the user logged out before leaving any workstation unattended, even for a brief period.
- Where 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 always kept as clear as possible; in particular Council information classified as 'WCC Confidential', 'Official Sensitive' 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.
- Users should not leave workstations or devices in ‘sleep mode’ for convenience.

Please consult WCC’s **Accommodation Standards** for more detail

Please consult WCC’s **Information Handling and Safe Haven** procedure for more detail

6. WCC Devices (WCC owned assets)

Mobile device computing (which includes Surface Pros, laptops, mobiles, and tablets) within WCC has enabled flexible working practices intended to improve work/life balance. However, mobile devices also create information security risks for WCC.

WCC needs to ensure that information assets and systems, used to access WCC information, are adequately protected with logical, physical, and environmental controls when being used by remote/mobile employees.

WCC information classified as ‘Official’, ‘Official Sensitive,’ ‘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.**

Remote and mobile workers are responsible for ensuring that information held locally is backed up regularly to the WCC network or OneDrive, based on the importance of their data. If backup via the WCC network is not available or feasible then they must discuss this with their line manager and where necessary, involve ICT.

For WCC mobile devices, which includes laptops, mobiles and tablets, please consult the WCC **Mobile Device Policy.**

For non-personal devices and non-managed WCC devices staff are advised to consult WCC’s **Unmanaged Laptop Policy** for more detail.

For personal devices please consult the “**BYOD – Bring Your Own Device**” section within this document.

7. BYOD - Bring Your Own Device

The purpose of this section is to help users understand their responsibilities when using their own devices when connecting to any WCC infrastructure or WCC assets.

- Do not store any WCC information in any location other than explicitly WCC allowed locations, this includes storing data on a non-WCC device or personal public cloud environment.
- When using WCC cloud environments, such as Microsoft Office 365 and Azure, staff must sign in and sign out, when finished. Under no circumstances are staff to use any ‘remember/save password’ functionality that may be offered to them.
- If staff are using their own device, to access WCC resources/information, staff must ensure their device is regularly updated to the latest version, including all other apps and programs.

Please consult WCC’s **Bring Your Own Device Policy**

For non-personal and non-managed WCC devices it is advised to consult WCC’s **Unmanaged Laptop Policy** for more detail.

8. Removable Media Devices

WCC recognise that removable media is used for the storage and transfer of WCC data. In order to protect this data and remain compliant with the Data Protection Act (DPA) and General Data Protection Regulation (GDPR), the data must be secured in transit. To simplify this process, only approved encrypted devices will be offered to staff and controls to stop data being removed on unapproved devices will be implemented.

Staff MUST NOT use an unapproved device for the storage of ANY WCC data. Any data found to be residing on unapproved i.e. unencrypted, USB storage devices MUST be immediately removed.

The Removable Media Policy sets out what is acceptable and what controls are to be implemented and how they must be used to protect WCC data while in transit on a removable media device.

Please consult WCC’s **Removable Media Policy** for more detail.

9. Encryption (Cryptography)

Cryptography allows data to be secured by making it unreadable, providing confidentiality, to parties that do not know the decryption key. Cryptography also allows integrity, authentication, and non-repudiation to be achieved.

The GDPR and the DPA require that companies implement appropriate technical measures to secure data. This includes at rest and in transit and cryptography is a method that allows this to be achieved. Sometimes it is used to provide integrity to data that may be freely and publicly read but must be accurately transmitted and stored.

There are legal requirements under the GDPR and Data Protection Act where data must be secured in transit, exceptions on this basis cannot be made.

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

Please consult WCC's **Cryptography Policy** for more detail.

10. Acceptable Use

The Acceptable Usage Policy titled "Email, Internet and Social Media Policy" covers the security and use of all WCC's information and IT equipment. It also includes the use of email, internet, social media, voice, and mobile IT equipment.

Please consult WCC's **Acceptable Use Policy (Email, Internet and Social Media Policy)**

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, social media 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.

Please consult WCC's **Acceptable Use Policy (Email, Internet and Social Media Policy)**

11. Security Incident Management

WCC recognises that from time to time 'things go wrong' and there may be a breach of security involving information or equipment holding information. The purpose of the "Data Breach and Information Security Incident Procedure" is to ensure that all actual or potential information security incidents are reported centrally to enable WCC to react quickly and effectively to minimise the impact.

These procedures are **mandatory** and must be followed by all staff as part of the council's Information Governance Framework which is the standard for managing information in the council and is one of the linked procedures in the **Information Compliance Policy** aimed at all staff.

Please consult WCC's **Data Breach and Information Security Incident Procedure** for more detail

12. Starters and Leavers Data Access

With access now available to a wide array of systems, it is vital to have a correct and secure process 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.

Please consult WCC's **New Starter Setup guidance** for more detail about new starter set up.

13. Third Party Access

There are times when third parties need to access to WCC managed systems including internal networks. WCC takes the security of remote access very seriously as accidental or deliberate misuse of WCC property or data could result in a breach of confidentiality, integrity or availability and in exceptional circumstances result in legal issues for WCC. A Data Protection Impact Assessment (DPIA) would very likely be required to ensure access is provided lawfully and only to those with a business requirement to do so.

This policy is designed to assist all staff in understanding their responsibilities when dealing with any 3rd Party (including external vendors and suppliers) that require any access to the WCC network and ICT assets.

Please consult WCC's **Third Party Remote Access** Policy for more detail.

14. Internet of Things (IoT) and Smart Devices

IoT and Smart Devices are pieces of equipment that have a stripped down and barebones operating system that can connect to the internet. These can include, but are not limited to, smart lighting, thermostats and building alarms.

The "Internet of Things and Smart Devices Security Policy" aims to ensure any IoT and Smart Devices that WCC use are secure and do not introduce unnecessary risks into WCC networks and as such pose a risk to WCC data. No devices of this nature can be used within WCC until authorised by the Cyber Security Manager. A DPIA (Data Protection Impact Assessment) and SSRA (System Specific Risk Assessment) would be required before any approval would be given by CSM, DPO, and in some cases SIRO).

Please consult WCC's **Internet of Things and Smart Devices Policy** for more detail.

15. Cloud Policy

The Cloud Security Policy details the WCC cloud security position and outlines elements that must or should be adhered to when dealing with cloud environments. Specific cloud provider settings are not detailed within the Cloud Security Policy so please contact the Cyber Security Team for specific cloud provider policy or guidance.

Please consult WCC's **Cloud Security Policy** for more detail.

16. Network Security Policy

The security of WCC networks is extremely important to maintain the necessary confidentiality, integrity and availability for WCC assets and data. The Network Security Policy details the security requirements that must be met for all WCC network devices throughout their lifecycle.

Please consult WCC's **Network Security Policy** for more detail.

17. Environmental Security

The "Office Accommodation Standards" is primarily a Facilities policy, but it also details all security requirements relevant to the physical environment at WCC.

Please consult WCC's **Office Accommodation Standards** for more detail

18. Firewall Management Policy

The Firewall Management Policy details requirements for all employees who have responsibilities for, or dealings with, the WCC Firewall infrastructure. Please contact the Cyber Security Team for access to this policy.

Please consult WCC's **Firewall Management Policy** for more detail

END OF POLICY