WICKLOW COUNTY COUNCIL
Comhairle Chontae Chill Mhantain

Acceptable Usage Policy

Revision History				
Release Date	**Version**	**Last Revised By**	**Classified**	**Revision Description**
5 July 2019	1.0	GDPR Governance Group	Internal	
5 October 2023	1.1	Paul Aurisch	Internal	
20 February 2024	1.2		Internal	

Approval History		
Date	**Version**	**Approved By**
26th November, 2024	Final version	Approved by Senior Management Team at meeting held on 26th November, 2024.

Table of Contents

1. Introduction

The purpose of this document is to outline the policy for the safe, professional and proper use of Wicklow County Council's (WCC) ICT systems and services. This policy applies to all users of ICT systems and services accessible by any users employed by WCC. This includes permanent and temporary staff members, elected members, committee members, independent contractors, subcontractors, staff of partner organisations or any user of ICT systems and services provided by WCC.

Users of the ICT systems and services are expected to abide by this Acceptable Usage Policy and all other appropriate policy documents. All users of WCC's ICT systems and services are expected to use these resources in an efficient, effective, ethical, moral, lawful and secure manner.

The policy applies to all use of computer and telecommunications resources and services which are provided, and/or subscribed to, by WCC including, but not limited to, any internal or external communications networks (Internet, commercial online services, instant messaging facilities, wireless communication facilities, SMS, MMS services, social media platforms, and electronic mail systems) that are accessed directly or indirectly from computer facilities and/or services for or by WCC.

This policy is designed to provide all users of WCC's ICT systems and services with guidance on their rights and responsibilities with respect to the correct use of ICT devices, systems and services. WCC has developed this Acceptable Use Policy to protect staff, service delivery, the public, and partners from accidental or deliberate misuse of the ICT systems and services.

Access to all WCC Information Technology (IT) systems, equipment and infrastructure is conditional on the acknowledgement and acceptance of this policy.

2. Overview

The ICT systems and services employed within WCC provide the Organisation with the opportunity to enhance the productivity of its workforce and to also provide for a better service. However, while providing numerous benefits, the ICT systems and services also present a number of risks that need to be managed.

A formal Acceptable Usage Policy allows users to understand their rights and responsibilities when using the ICT systems and services. It also allows WCC to implement and communicate the appropriate procedures to:

- Protect against potential disclosure of sensitive information.
- Protect against loss or theft of WCC equipment.
- Protect against corruption of sensitive information.
- Protect against litigation arising out of illegal or immoral use of WCC equipment.
- Ensure compliance with legal, government and regulatory requirements.
- Ensure protection of individual users of ICT systems and services from the inherent risks of ICT, such as disclosure of data, exposure to inappropriate material, cyber-attack and unnecessary system downtime.
- Respect the rights and privacy of others.
- Ensures WCC's IT resources are used for legitimate business purposes only.
- Protect against financial loss.
- Protect against reputational loss.

This policy document is intended to allow WCC to derive the benefits of increased efficiency associated with ICT systems and services while ensuring the protection of information assets, the integrity of WCC, and the protection of staff member rights.

This policy document is to be used in conjunction with other policy documents applicable to WCC, such as, but not limited to

- Wicklow County Council Password Policy
- Wicklow County Council Social Media Policy
- Code of Conduct for Employees January 20027
- Code of Conduct for Elected Members, published in July, 2019 and last updated 28th October, 2021.
- Wicklow County Council Disciplinary Policy and Procedure, May 2020
- Wicklow County Council Data Protection Policy reviewed 14th February, 2023.
- Wicklow County Council Anti-Fraud and Corruption Policy and Procedures, 2024
- Wicklow County Council Policy and Procedure on Protectecd Disclosures Internal Reporting in the Workplace January, 2024
- Wicklow County Council Policy and Procedure on Protected Disclosures External reporting to Chief Executive of a Local Authority as a prescribd person under SI 367 of 2020 January, 2024.

2.1 Policy Scope

This policy applies to all ICT systems and services that are owned, rented or leased by WCC. ICT equipment includes, but is not limited to the following:

- Computing devices such as desktop and laptop computers, tablets, thin client computer terminals, servers or printers.
- Mobile phones, including smartphones and other portable devices.
- Digital storage devices such as USB devices and digital cameras.
- Printing and scanning devices.
- Data/software/applications stored on WCC ICT systems and services.
- Network resources that are owned and maintained by WCC.

2.2 Not within Scope

This policy does not apply to:

- Computing equipment and related services that are not owned, rented, managed or leased by WCC.
- Any data, including pictures, documents, messages (e.g. WhatsApp, Gmail), etc, saved within personal profiles on phones and/or tablets, is the sole responsibility of the user.

2.3 Summary

The main points covered by this document are:

- Reasons for Acceptable Usage Policy.
- Scope of WCC Acceptable Usage Policy – what types of devices does this policy cover.
- The responsibilities that apply to WCC under the Acceptable Usage Policy.
- The responsibilities that apply to the users of ICT systems and services under the Acceptable Usage Policy.
- WCC's Acceptable Usage Agreement – that must be signed by all users of WCC's ICT systems and services before ICT services will be made available to them.

3. Acceptable Usage Policy

The following policy, rules and guidelines apply to all users of ICT systems and services provided by WCC. All ICT systems and services, and all material generated using these systems, including all associated backups, are considered to be assets owned by WCC, and WCC retains all rights, including intellectual rights, to that material.

WCC reserves the right to monitor all aspects of the ICT systems and services for the purposes of operations, maintenance, auditing, security or investigative functions.

Line management exception-based monitoring of the use of ICT systems and services must be authorised by a member of the Senior Management Team.

IT-based monitoring of user activity will occur where automated reporting systems indicate an alarm or alert that requires investigation.

Staff members involved in the monitoring of ICT systems and services are obliged to keep all details of the monitoring process confidential.

3.1 Wicklow County Council Responsibilities

Under the Acceptable Usage Policy, WCC is responsible for the following:

1. Informing all users of ICT systems and services of WCC's Acceptable Usage Policy and ensuring that all users of these systems can access and review any changes to the Acceptable Usage Policy.

2. Training IT network and system administrators in the correct and proper practices for ensuring the continued operation, security and maintenance of ICT systems and services.

3. WCC is obliged to keep abreast of any legal or legislative changes made in relation to data held on the Organisation's computing systems and the transmission of same. WCC will modify WCC's Acceptable Usage Policy as appropriate.

4. IT network and system administrators are charged with the responsibility for the administration, maintenance and security of the infrastructure to support ICT systems and services. However, end users are responsible for safeguarding and maintaining the integrity of the computing devices, together with the applications and data held therein, that are assigned to them.

5. IT network and system administrators are not authorised to monitor or view staff members' computing devices, their network connections or usage of any systems including electronic messaging systems, without the express permission of the user or having been authorised to do so by the Senior Management Team.

6. It should be noted that IT network and system administrators may monitor overall systems usage as part of their ongoing responsibilities for managing, securing, auditing and supporting ICT systems and services. However, this monitoring will be restricted to overall usage and aggregated data will be used for this purpose and will not be on an individual user basis unless

authorised to do so by a member of the Senior Management Team or the Information Security Officer.

7. IT network and system administrators are not authorised, unless requested by the user, the user's manager, the Information Security Officer or by Senior Management, to change the user's password so that the computing device or the related network traffic can be accessed.

8. WCC will provide a secure platform to enable access to WCC's network. This will enable the end user to access the Internet, electronic mail and authorised network resources. This secure platform will ensure that all data transmitted is secured to acceptable standards to protect its confidentiality and integrity.

9. All computing devices, services and systems will be password protected. Passwords must be in accordance with WCC's password policy. WCC may from time to time audit the quality of the passwords being used to ensure they are in compliance with WCC's password policy.

10. WCC will configure ICT systems and services to be protected at all times from unauthorised access and compromise. To this end, all WCC computing systems and devices will be configured in accordance with recognised vendor and industry best practices and guidelines. These practices and guidelines will be reviewed regularly.

11. Where appropriate, any password protection facilities in the computing devices, systems and services will be availed of.

12. As deemed necessary, the utilisation of Multi-Factor Authentication (MFA) capabilities within the systems and/or services is mandatory.

13. Computing devices and systems will also be configured to be regularly updated with the latest operating system and application patches and updates.

14. WCC will protect the integrity of its network by ensuring only authorised devices can connect to the network. In addition, only authorised devices that have the latest security updates, virus signatures and software updates will be allowed access to the Organisation's network.

15. WCC data held on computing systems and devices must be protected from malicious software, such as computer viruses, at all times. To this end, all WCC's computers will be configured with anti-virus software. This software will be configured to accept updates on a regular basis. Where appropriate, certain computers will also have additional security software installed.

16. Only authorised peripherals, such as printers, cameras, USB devices and scanners, will be attached to any computing device. Where possible, WCC will implement a solution to restrict attachment to only authorised peripherals.

17. All data generated and processed by computing devices and systems must be saved regularly onto the network so that it can be backed up. Data stored on a user's local device (desktop, C:\ drive, etc.) will not be covered by WCC's backup solution. It is the user's responsibility to ensure data retrieval in case of device loss or hardware failure. Users must save necessary data on network drives for backup. For inquiries or guidance, contact WCC's IS Service Desk.

18. Data will at all times be stored securely on the Organisation's data processing systems. Confidential data will not be stored on computers without appropriate protections being in place. To this end any confidential data stored on user computers, such as mobile computers, will be encrypted using an industry standard algorithm authorised by WCC. The encrypted data can only be accessed by either the authorised user, the user's line manager or by a network or systems administrator authorised to do so by a member of the Senior Management Team.

19. WCC will, at all times, meet its obligations as per legal requirements to protect the privacy of its staff and elected members. Only in exceptional circumstances, authorised by the Senior Management Team, will staff usage of email, electronic messaging, computing or online systems be monitored.

20. WCC reserves the right to restrict the sending and receiving of certain types of files and/or file attachments. This is to ensure that WCC is not in breach of any copyright laws, protects employees from content that is unlawful, indecent or immoral, and ensures that essential network resources, such as bandwidth, are not consumed unnecessarily.

21. WCC reserves the right to implement systems to control and restrict access to certain websites, electronic messaging and online services. At all times the service will comply with its obligations and responsibilities outlined in this policy document. These systems to control and restrict access will be in place 24/7 and not solely during working hours.

22. WCC's Information Systems (IS) Section will develop a security awareness program for all of its users and elected members.

23. WCC's ICT systems and services are provided primarily for WCC business-related purposes.

24. WCC does not accept liability for any fraud, theft or information loss that results from a user's personal use of WCC's Information Technology resources.

3.2 Responsibilities of Computing Users

Users of WCC's ICT systems and services should be aware and comply with their responsibilities under WCC's Acceptable Usage Policy and all other relevant policies impacting on information security. This includes reading, understanding and adhering to WCC's Acceptable Usage Policy and other relevant policies impacting on information security.

1. Use of WCC's ICT systems and services and peripherals is bound by this policy and other relevant policies deemed appropriate.

2. WCC will provide only authorised users with access to ICT systems and services. Enhanced security measures, including Multi-Factor Authentication (MFA), geolocation restrictions, access policies and other technologies will be implemented as needed to ensure secured access.

3. WCC reserves the right to withdraw the provision of ICT systems and services where due care is not taken in regard to the assigned devices, services and/or systems. This may also result in the user being subject to disciplinary action.

4. WCC reserves the right to withdraw access to the Organisation's ICT systems and services where in the opinion of WCC inappropriate use of these systems or breach of the Acceptable Usage Policy has occurred. This may also result in the user being subject to disciplinary action up to and including dismissal.

5. The ICT systems and services are provided for business use. Usage of ICT systems and services may be monitored by WCC and disciplinary action may be taken where abuse is identified.

6. Users of ICT systems and services will not use profane, abusive, derogatory or obscene remarks in any communications about fellow staff members, members of the public, and staff from other organisations, suppliers and/or clients.
7. Users will lock or log off their workstation when leaving it unattended.
8. Users of ICT systems and services will comply with WCC's Code of Conduct.
9. Users will use ICT systems and services in accordance with the Council's Health and Safety Procedures.
10. All ICT systems and services acquired for or on behalf of WCC shall be deemed to be WCC property. Each staff member issued with a computing device is responsible for the security of that device, regardless of whether the device is used on WCC property/locations, at the staff member's place of residence, or in any other location such as a hotel, conference room, car or airport.

11. The staff member to whom the computing device is assigned is fully responsible for the safety of the data and the hardware. All precautions must be taken by the staff member to prevent theft, breakage and unauthorised access. Where the staff member does not take such precautions, the staff member may be held responsible for the loss/theft/vandalism of the device.
12. Users will not attempt to disable or circumvent any security controls or procedures implemented by WCC.
13. Only authorised users of WCC may use ICT systems and services and data. These may only be used in accordance with their duties. Any authorised staff member providing access to their computing device to unauthorised users will be in breach of the Acceptable Usage Policy and may be subject to disciplinary action.
14. Users are responsible for informing management of any abuses of the Acceptable Usage Policy.
15. Users must ensure that accessing email and other online files is only as authorised and in the performance of the user's job function.
16. Any user who discovers a "security issue" in any system allowing them to access information they are not authorised to, should report the incident to their line manager and the Information Systems Section.
17. Users will not store or send fraudulent, harassing, embarrassing, indecent, profane, obscene, pornographic, intimidating, terrorist, paramilitary or other unlawful material using the ICT systems and services provided by WCC.

18. Users should note that spam emails/messages should never be responded to as this simply confirms their email address is a legitimate address. All spam email should be ignored and deleted.
19. Users should be aware that sending emails to groups of people through the TO or CC fields exposes the email addresses of those individuals addressed. Users should consider using the BCC field.
20. Users will not access indecent, profane, obscene, pornographic or other unlawful material using ICT systems and services provided for by WCC.
21. Users will not download or install any software onto any computing device other than that authorised by WCC. The installation of unauthorised software could expose WCC to virus attack or potential breach of copyright law. Any unauthorised software will be removed, and the user may be subject to disciplinary action.
22. Only authorised peripheral devices installed by WCC may be used on the user's computing device. Any unauthorised peripherals will be removed and the user may be subject to disciplinary action.
23. Unless authorised by the IS Section, users are strictly prohibited from connecting personal or unauthorised devices to the network or any technology or service owned, leased or licensed by WCC.
24. Users will not store or send any material on ICT systems and services that is in breach of software licenses and/or copyright. Users should be aware that copyrighted material can and does include text, picture, video, music and sound files, as well as executable code. Any material discovered on a user's computing device that is in breach of software licenses and/or copyright will be removed, and the user may be subject to disciplinary action.
25. The ICT systems and services of WCC may not be used for the transmission of commercial advertisements, solicitations, electronic chain letters, promotions, destructive programs (such as computer viruses, Trojan and/or self-replicating code), political, pornographic and/or illegal material. Users receiving such material shall inform their supervisor or manager immediately.
26. Users will not send WCC data or information to third parties if this is not in accordance with the Organisation's information handling policies.
27. Users will at all times comply with the relevant Data Protection legislation and the direction of the Data Protection Officer.
28. If a user suspects that their computing device or communications are being monitored, they will notify their immediate supervisor, the Information Security Officer or a member of the Senior Management Team.
29. If a user suspects that their device has been compromised or accessed without permission, they will notify their immediate supervisor and the IS Support Desk.
30. WCC reserves the right to require that computing devices be returned at any time. The staff member must return the device and any associated peripherals, data and software to their immediate supervisor or their manager within 24 hours of the request.
31. Upon termination of employment or job reassignment , the computing device, any data held on that device and any peripherals must be returned immediately to the user's immediate supervisor or to the HR Department.

32. Users who misplace, lose or have a computing device stolen will notify their immediate supervisor and the IS support desk immediately when the device is discovered missing.

33. Users will not discuss the security mechanisms employed by WCC to protect its computing resources with any unauthorised persons. Unauthorised persons are people who are not staff members of WCC and staff members who are not authorised to use the computing platform.

34. Users of ICT systems and services will not use these systems to deliberately waste their own time and that of their colleagues. This includes:

    - Playing games.
    - Accessing non-business related services and websites.
    - Uploading/downloading large unofficial files that create unnecessary non-business related loads on network traffic.
    - Accessing streaming audio/video files, for example, listening to music or watching movie clips online.
    - Accessing online gambling sites.
    - Accessing online personal email accounts.
    - Forwarding audio/video files to colleagues.
    - Participating in mass non-business related mailings such as chain letters.
    - Sending unofficial attachments.

35. Users of ICT systems and services should be aware that third party systems, outside the confines of WCC, are not secure. Users will not give out more information than is necessary to fulfil the purpose of the task in hand. No confidential or sensitive information, personal information or information relating to the Organisation's IT systems or resources should be disclosed without express authorisation from the Information Security Officer.

36. It is the responsibility of all users of ICT systems and services to assess the validity of the information found on external networks such as the Internet. Information contained on such networks can range from sources that are reliable, to those that are controversial, unsubstantiated and offensive.

37. All users of ICT systems and services will comply with all current laws, government regulations and any regulatory requirements.

38. WCC computing devices, systems and peripherals will be configured according to the Organisation's standards. Users shall not make changes to the standard installation, shall not modify the hardware and software configuration, and shall not modify the Operating System. All requests for system changes must be authorised by the IS Section. These standards may be revised periodically to reflect changes in legislative requirements and the evolving landscape of cybersecurity.

39. Users will not attempt to access any data or programs contained on WCC's ICT systems and services, or connected to WCC's ICT systems and services, for which they do not have authorisation or explicit consent of the owner of the system, data or program or relevant manager.

40. Users will not download, install or use any software tools that are designed for hacking, discovering passwords, discovering security holes or weaknesses in WCC's ICT systems and services or networks, unless explicitly authorised to do so by the Information Security Officer.

41. The use of social media apps for work purposes is strictly forbidden under the Acceptable Usage and Data Protection policies. Only approved WCC social media accounts such as WCC Linkedin, WCC Facebook WCC Instagram accounts and WCC X can be used, by authorised staff, on behalf of the Council.
42. WCC electronic devices and computing, online and messaging systems are provided strictly for business use. As such, users will not use WCC electronic devices, computing, online and messaging systems for personal use or for conducting business activities not related to, or authorised by, WCC.
43. All work-related communication on WCC provided mobile devices must be via WCC approved apps in the Work profile.
44. Users must not use their WCC email address/username/ID for registering on websites unless instructed to do so as part of their work duties.
45. Users must ensure use of all ICT systems and services complies with the requirements of GDPR and related Data Protection Legislation and FOI Acts.
46. WCC's Manage Print Service uses the "follow me" print model which means that documents are only printed when the user authenticates at a printer. Printouts containing confidential or personal information should be immediately removed from the printer. Once documents are released to print, the user must ensure that the documents are securely removed.

4. Password Management Guidelines

Your password is personal to you and should not be shared with others. You are responsible for all activity carried out on the network using your user ID. If you discover that your password is known by someone else, you should change it immediately and report this to the Information Security Officer (wcc-security@wicklwococo.ie or wccsecurity@wicklwococo.ie) and the IS Help Desk (issupport@wicklowcoco.ie).

Do not use passwords that are easy to guess, such as names, place names, etc. Ideally, your password should consist of a mixture of text and numbers. To make your password even more secure, you should mix the case.

Please refer to the WCC Password Policy for guidelines on managing passwords.

5. Acceptable Usage Agreement – The acceptable usage policy will be provided to all new staff recruited to Wicklow County Council on day of induction by HR and the signed acceptable use agreement will be returned within a period of 2 days to their line manager for submission to HR Officer for retention on file. This acceptable usage agreement will also be circulated to all existing staff for signing and submission to their line manager for onward submission to HR for retention.

I have received a copy of Wicklow County Council's Acceptable Usage Policy, dated 26th November, 2024. I recognise and understand that Wicklow County Council's ICT systems and services are to be used for conducting Wicklow County Council business only.

I have read and understood the aforementioned document and agree to follow all policies and procedures that are set forth therein. I further agree to abide by the standards set in the document for the duration of my employment with Wicklow County Council.

I am aware that violations of this Acceptable Usage Policy may subject me to disciplinary action.

I further understand that my use of the ICT systems and services reflect Wicklow County Council, to fellow and potential staff members, the public, organisations and suppliers. Furthermore, I understand that these documents can be amended at any time, and it is my responsibility to keep myself abreast of any changes to this document.

_____ _____

Staff member Signature Date

_____

Staff member Printed Name

_____ _____

Line Manager Signature Date

Received in HR on _____