Wireless Network Policy

1 Version History details and author

1.0	27/10/2010	Completed for distribution	Jo White
1.0	24/11/2010	Approved by Information Governance Group	Jo White
2.0	23/11/2011	Reviewed by Information Governance Group	Jo White
3.0	19/12/2012	Reviewed by Information Governance Group	Jo White
4.0	10/02/2014	Reviewed by Information Governance Group	Jo White
5.0	16/03/2015	Reviewed by Information Governance Group	Jo White
6.0	04/04/2016	Reviewed by Information Governance Group. No changes.	Jo White
7.0	09/05/2017	Reviewed by Information Governance Group. Transformation changed to ICT.	Jo White
8.0	11/06/2018	Reviewed by Information Governance Group. No changes.	Jo White
9.0	06/08/2019	Reviewed by Information Governance Group. Head of ICT changed. GCSx removed.	Jo White
10.0	11/08/2020	Reviewed by Information Governance Group. Addition of Council's wifi encryption standard.	Jo White
11.0	07/09/2021	Reviewed by Information Governance Group. No changes.	Jo White
12.0	08/11/2022	Reviewed by Information Governance Group. No changes.	Jo White
13.0	12/12/2023	Reviewed by Information Governance Group. Agency staff added. Audit Services penetration testing paragraph removed.	Jo White
14.0	14/01/2025	Reviewed by Information Governance Group. Explanation of wireless LANs expanded. Wireless network testing now part of IT Health checks.	Jo Williams

This document has been prepared using the following ISO27001:2022 standard controls as reference:

A.5.15 - Access control
A.5.17 - Authentication information
A.5.36 - Compliance with policies, rules and standards for information security
A.5.37 - Documented operating procedures
A.8.8 - Management of technical vulnerabilities
A.8.20 - Networks security
A.8.21 - Security of network services

2 Introduction

2.1
Wireless Local Area Networks (LANs) form part of the Council's corporate network infrastructure. In order to protect the business needs of the Council the wireless network must meet the same level of security employed by the rest of the infrastructure.

This policy is to ensure that the deployment of wireless networking is controlled and managed in a centralised way to provide functionality and optimum levels of service whilst maintaining network security.

The intention of this policy is to define roles and responsibilities for the design of any emerging wireless network, the installation, registration and management of wireless access points and devices, adequate management allocation of the wireless frequency spectrum and the services offered to end users for wireless access.

The Council's WiFi network is encrypted using WPA2 to provide secure authentication based on the Advanced Encryption Standard (AES).

3 Purpose

3.1 This policy outlines a common set of procedures and operational criteria for the effective management of 802.11 wireless LANs conforming to accepted technical standards (IEEE 802.11x). Due to the characteristics of Wireless technology, all wireless developments must be planned, deployed and managed in a carefully controlled manner, and developed in accordance with the Council's Information Security Policy.

The three main areas that the wireless policy will address include:

Security - Wireless LANs offer connectivity to anyone within range of an Access Point; physical boundaries are no longer a relevant option for preventing access to the network. Installations of non-approved devices which may be configured with little or no security increase the risk of a breach of security of the Council's data network and are prohibited.

Non-Standard Devices - Non-standard or misconfigured wireless devices can cause disruptions to the wireless LANs and subsequently the wired network. The Council therefore prohibits the installation of any non-standard wireless access points. Only wireless network equipment authorised and installed by Digital Services is permitted on the Council's network.

Interference – Wireless technology compliant with the 802.11 standards uses frequencies from a band which is divided into channels. In order for adjacent access points to work with each other and not cause interference or performance issues, a different channel must be used for each Access Point.

4 Policy Statement

4.1 Scope
This policy applies to all areas of wireless connectivity to the Council's network infrastructure, and includes all wireless devices operating within the Council's IP

address range, on any of the Council's premises, or any remote location directly connected to the Council's data network. The policy describes the standards that users are expected to observe when using the Council's wireless facilities and details the potential consequences for misuse.

Digital Services is responsible for the Council's network infrastructure. The wireless network is an extension to this network and therefore Digital Services has the responsibility for the design, deployment and management of the Council's wireless LANs.

4.2 Policy Restrictions

i. All Access Points and wireless devices used by staff on the Council's secure wireless network must conform to all related national regulations, standards and recommended specifications as defined by Digital Services
ii. All new Access Points and wireless devices used by staff on the Council's secure wireless network must be purchased and installed by Digital Services, in-line with the Council's current purchasing policy and IT Standards.
iii. All Access Points and wireless devices used by staff on the Council's secure wireless network must follow the Digital Services standard configuration settings.
iv. The installation of any non-standard Access Points or wireless devices is prohibited.
v. Digital Services has the right to disable any non-standard, unauthorised devices which may cause interference with existing approved Access Points or devices. Such devices may be removed without prior notice.
vi. Monitoring of wireless networks is undertaken by Digital Services on a regular basis.
vii. Wireless security testing will be performed on a periodic and random basis using audit penetration tests involving skills and tools commissioned from independent third party companies. The use of unauthorised wireless security testing on the Council's network is considered a disciplinary matter up to and including gross misconduct.
viii. New requests for the installation of new Access Points or wireless devices must be directed through Digital Services.
ix. Unauthenticated open access to the Internet may be provided separately from the secure wireless network via wireless hot spots in the Council's public buildings. Access via personal laptops and other mobile devices will be subject to internet filtering.

4.3 Appropriate Use

The Council supports the appropriate and proper use of services and facilities that it provides to staff and other authorised users. Only Council approved software and hardware devices are permitted on the Council's secure wireless network.

Failure of contractors, agency staff, partners/agencies or third party organisations to comply with this policy may result in termination of contracts and connections, suspension of services and where appropriate, in accordance with the terms of individual contracts and agreements, the Council may also seek to recover any loss incurred as a result. Where the Council considers it appropriate, inappropriate use of the Council's wireless facilities will be reported to the police.
Failure of employees to comply with this policy may result in disciplinary action being taken.

4.4 Regulatory Framework

The Council takes responsibility for providing an appropriate regulatory framework, including specific standards and guidance relating to the appropriate use of these Council services and facilities. The Wireless Network Policy constitutes a component part of this framework.

Business use of all ICT facilities provided by the Council is subject to the relevant Policies and Regulations, in particular the Council's Internet and e-mail policy, Safe Haven, Information Security policy and Acceptable Use policy.

4.5 Acceptance

All users of information and ICT systems for which the Council is responsible must agree to, and abide by, the terms of Derbyshire County Council's Acceptable Use Policy, associated security policies and applicable Codes of Connection and Conduct.

5 Roles and Responsibilities

5.1
All Wireless LANs are monitored and maintained by Digital Services. Any Access Point or wireless device which is connected to the Council network infrastructure becomes the responsibility of Digital Services.

5.2 User responsibilities

Users of the Council's secure wireless network must not connect any unauthorised equipment to the Council data network without prior approval from Digital Services. If Digital Services deems that any particular equipment may be the cause of unacceptable degradation of the performance of the network or poses a security risk, then the user must co-operate with the disconnection of that equipment from the network.

All users accessing authorised wireless equipment must abide by the Council's Acceptable Use Policy, associated security policies and applicable Codes of Connection and Conduct.

Apart from notification of the availability of the guest "Open" wireless network, no information regarding the wireless network, including configuration and setup information, should be shared with any unauthorised users, third party vendors or members of the public.

The Council's wireless network must not be used inappropriately to send, receive or make available data or information that may be classified as offensive, obscene, indecent or illegal.

6 Breaches of policy

Breaches of this policy and/or security incidents can be defined as events which could have, or have resulted in, loss or damage to Council assets, or an event which is in breach of the Council's security procedures and policies.

All employees, elected members, partner agencies, agency staff, contractors and vendors have a responsibility to report security incidents and breaches of this policy as quickly as possible through the Council's Incident Reporting Procedure. This obligation also extends to any external organisation contracted to support or access the Information Systems of the Council.

In the case of third party vendors, consultants or contractors non-compliance could result in the immediate removal of access to the system. If damage or compromise of the Council's ICT systems or network results from the non-compliance, the Council will consider legal action against the third party. The Council will take appropriate measures to remedy any breach of the policy through the relevant frameworks in place. Where it becomes apparent that there may have been a breach of this policy by an employee then the matter may be dealt with under the disciplinary process.

This document is owned by the Information Governance Group and forms part of the Council's ISMS Policy and as such, must be fully complied with.