Public Internet Access Policy

1 Version History details and author

1.0	21/12/2010	Completed for distribution	Jo White
1.0	25/01/2011	Approved by Information Governance Group	Jo White
2.0	29/02/2012	Reviewed by Information Governance Group	Jo White
3.0	27/03/2013	Reviewed by Information Governance Group	Jo White
4.0	07/04/2014	Reviewed by Information Governance Group	Jo White
5.0	11/05/2015	Reviewed by Information Governance Group. Extra line about monitoring.	Jo White
6.0	09/01/2017	Reviewed by Information Governance Group	Jo White
7.0	05/02/2018	Reviewed by Information Governance Group. No changes.	Jo White
8.0	04/03/2019	Reviewed by Information Governance Group. Public code of conduct removed. Updates to filtering and controls added.	Jo White
9.0	03/03/2020	Reviewed by Information Governance Group. No changes.	Jo White
10.0	13/04/2021	Reviewed by Information Governance Group. No changes.	Jo White
11.0	10/05/2022	Reviewed by Information Governance Group. No changes.	Jo White
12.0	06/06/2023	Reviewed by Information Governance Group. No changes.	Jo White
13.0	11/06/2024	Reviewed by Information Governance Group. Agency staff added.	Jo White

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

ISO Control A.5.10 - Acceptable use of information and associated assets
ISO Control A.8.20 – Networks security
ISO Control A.8.21 - Security of Network services

2 Introduction

As part of its public service duties, Derbyshire County Council provides free public access to the Internet for informational, educational and leisure needs. Sites where such facilities exist are libraries, learning establishments, guest wireless access points at designated locations, residential establishments and children's homes. When providing the public internet access facility, Derbyshire County Council recognises its obligation to protect public and Council information, equipment and systems from threats posed via the internet, malicious conduct and accidental occurrences.

This policy details the reasoning for vigilance and the required necessary standards/guidelines with regard to security, when enabling and using public internet access.

3 Purpose

The purpose of this policy is to establish the standards and guidelines by which public internet access will be provided. This will enable systems, data and equipment of both the Council and the public to remain as secure as possible. When using publicly available internet access, all council employees, contractors, vendors and members of the public should adhere to this policy.

4 Scope

The scope of this policy includes:-

- ICT equipment and systems belonging to, or under the control of Derbyshire County Council
- Information in use on Council ICT equipment, networks and systems.
- ICT equipment and systems belonging to members of the public using the Council's public internet facilities.
- The rules, regulations, software and hardware controls incorporated into the provision of public internet access.
- Internet content viewed, copied or circulated by all parties utilising the Council's public internet access.
- All parties who use public internet access or parties who enable public internet access, include but not limited to:

    - Council employees
    - Elected Members
    - Third Parties
    - Temporary staff
    - Agency staff
    - Partner organisations
    - Members of the public
    - Volunteers

5 Responsibilities

The Council will take all reasonable steps to provide ICT equipment and software with the correct security provisions either as a publicly available PC or as a 'hotspot' at agreed locations.

Members of staff are responsible for ensuring that equipment is used by the public in accordance with the Council's ICT Acceptable Use policy and adherence to this policy - therefore enabling internet access whilst minimising security risks.

Members of staff using Council provided equipment for internet use are required to adhere to this policy and the Council's ICT Acceptable Use policy.

Members of the public, staff, residents who utilise 'Guest' wireless access points or specially provisioned networked access points whilst using their own ICT equipment should be made aware of this policy – including any damage to privately owned ICT equipment resulting from incorrect usage is their responsibility.

The Council cannot be held responsible for any financial loss or damage incurred as a result of Internet activity.

Internet content viewed on Council owned equipment is passed through a filtering mechanism to control access to inappropriate information but the Council cannot be held responsible for that content.

Users should be aware that the Internet is not a secure medium and that third parties may be able to obtain information regarding users' activities.

6 Policy statement

With the Council's increasing provision of internet access to the public, it is essential that the security and integrity of information and systems is maintained and that the use of internet access facilities in libraries is provided on the basis of a prohibition against the creation, accessing, copying, storing, transmitting or publishing of any material that:-

- *is sexually explicit or obscene;*
- *is racist, sexist, homophobic, defamatory, harassing or in any other way discriminatory or offensive;*
- *possession of which would constitute a criminal offence;*
- *is criminal or illegal, or promotes criminal or illegal activities;*
- *contains images, cartoons or jokes that will cause offence*.

All activity and internet connections managed by the Council are monitored and recorded. Misuse of the facility could result in services being withdrawn or the content of an individual's activity being reported to the Police.

Copies of this policy and advice below should be clearly displayed in areas where public access to the internet is made available.

It is illegal to create, access, copy, store, transmit or publish any materials that fall into the following categories:-

- *National Security: instructions on bomb-making, illegal drugproduction, terrorist activities.*
- *Protection of Minors: inappropriate forms of marketing, displays of violence or pornography involving minors*

- *Protection of Human Dignity: incitement to racial hatred or racial discrimination, harassment.*
- *Economic Security: fraud: instructions on pirating credit cards.*
- *Information Security: malicious hacking.*
- *Protection of Privacy: unauthorised communication of personal data, electronic harassment.*
- *Protection of Reputation: libel: unlawful comparative advertising.*
- *Intellectual Property: unauthorised distribution of copyrighted works, e.g. software or music.*

In libraries, prior to use of the public internet service, users will be obliged to read and accept the terms of use as above. Users should be aware that the Council has the ability to monitor the use of public internet access facilities and the misuse of the facility could result in services being withdrawn or the content of an individual's activity being reported to the Police.

All Council owned equipment designated for use as public internet access systems are secured against theft and damage in accordance with the Council's ICT Security policy, installed with malicious code protection software in accordance with the Council's Malicious software and anti-virus procedures and be recorded on the Council's asset database with an assigned asset tag.

Any member of the public found maliciously interfering with either the Council's IT equipment or software used to enable public internet access may be barred from subsequent use of any of the Council's Internet Service's ICT facilities. Dependent upon the nature of the incident the matter may also be referred to the Police.

The use of public internet equipment by Council staff to process Council information is prohibited, except in exceptional circumstances and with line management approval.

Privately owned devices may be used to connect to filtered 'Guest' wireless access points at designated Council properties or facilities. No other method of connection is permitted from privately owned devices.

The Council have implemented appropriate controls to prevent users of the public internet service accessing, installing software or additional hardware on the Council's equipment.
The public IT equipment is returned to a default configuration setting on termination of a user session, including the removal of all personal identifiable data.

Council equipment available for use by the public has hard drive access removed. Whilst USB ports and read/write CD and DVD drives are accessible they are configured in such a way to stop software being installed onto the Council's IT equipment.

7 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 Public or Council assets, or an event which is in breach of the Council's security procedures and policies

All employees, temporary/agency staff, volunteers, elected members, partner organisations, 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 inappropriate use by a member of the public then access rights to the public internet facility may be temporality suspended or permanently removed dependent upon the level of breach that has occurred. In all instances, where potential criminal activity is suspected\reported the matter will be reported to the Police.

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. In the case of an employee then the matter may be dealt with under the Council's disciplinary process.

8 Compliance with legal obligations

Derbyshire County Council is bound by the regulations of the Data Protection Act (2018) including the UK General Data Protection Regulations (UKGDPR) and will not release information concerning the use of specific internet resources by any party except as required by law.

The Computer misuse act (1990), The copyright, designs and patents act (1988) the regulation of investigatory powers act (2000) will also apply to equipment used via the Public internet access provision.

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.