NWSLC

NORTH WARWICKSHIRE & SOUTH LEICESTERSHIRE COLLEGE

IT Acceptable Use Policy 2025/26(v3)

North Warwickshire and South Leicestershire College

Author: Director of IT

Target Audience: Staff / Student / Public

Policy Location: Staff SharePoint / Student Moodle / College Website

Contents

Acceptable Use Policy 2025/26(v3)

Page

1. Purpose 1
2. Scope 1
3. Associated Documents 1
4. Acceptable Use 1
5. Unacceptable Use 2
6. Security and Privacy 2
7. Software 3
8. Monitoring and Enforcement 3
9. Acknowledgement and Agreement 3
10. Equality Analysis 4
11. Data Protection Impact Assessment 4
12. Policy Monitoring and Review 4

Document History

Version Number	Amended By	Date of Revision	General Revision Description
V1.0	RODIS	01/11/2023	New Acceptable Use Policy to align with changes in KCSIE guidance
V2	RODIS	20/11/2024	Confirmed with Safeguarding, no updates required.
V3	RODIS	29/09/25	Confirmed with Safeguarding, Added AI misuse

Acceptable Use Policy 2025/26(v3)

1. Purpose

1.1. The NWSLC (The College) provides information systems and networks to support its educational and administrative activities. The purpose of this Policy is to ensure that these resources are used in a responsible, ethical, and lawful manner, and to protect the confidentiality, integrity, and availability of the College's information assets.

1.2. All users must be familiar with and comply with this Policy. Infringements of this Policy may lead to disciplinary action (up to and including immediate termination of employment/engagement/student enrolment) against individuals under the College's disciplinary procedures. Infringement of this Policy may also result in legal action and criminal proceedings against the College and/or individuals.

1.3. This Policy is non-contractual and may be altered by the College at any time.

1.4. This electronic version is the definitive version of the Policy.

2. Scope

2.1. This Policy applies to all students, faculty, staff, and other individuals who use the College's information systems and networks, whether on or off-campus, and regardless of the device or medium used to access them.

3. Associated Documents

3.1. BYOD Policy.

3.2. GDPR Policy.

3.3. Information and Technology Security Policy.

3.4. Online Safety Policy.

3.5. Safeguarding & Protecting Children and Vulnerable Adults Policy v2.

3.6. Staff Code of Conduct.

3.7. Staff Disciplinary Policy.

3.8. Student Conduct Expectations Policy.

3.9. Student Disciplinary Policy.

3.10. Keeping Children Safe in Education

3.10 Other policies and documents may be identified from time to time as circumstances change and may be added to this list.

4. Acceptable Use

4.1. The College's information systems and networks may only be used for activities that support the College's educational and administrative mission. Examples of acceptable use include:

i. Conducting research, accessing educational materials, and participating in online courses.

ii. Communicating with faculty, staff, and other students in a professional and respectful manner.

iii. Completing administrative tasks such as registering for classes, paying fees, and accessing personal records.

iv. Using the college's resources for academic and professional development.

5. Unacceptable Use

5.1. The following activities are strictly prohibited and may result in disciplinary action, including but not limited to suspension, expulsion, termination of employment, and legal action:

i. Using the College's information systems and networks for commercial purposes or personal financial gain.

ii. Engaging in activities that violate local, or international laws or regulations. In doing so you may be subject to disciplinary procedures or even prosecuted by law (Computer Misuse Act 1990).

iii. Accessing, using, or distributing copyrighted or proprietary materials without permission.

iv. Engaging in harassment, bullying, or any other form of discriminatory behaviour.

v. Creation, accessing, or transmission of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material.

vi. Creation or transmission of material with the intent to defraud or which is likely to deceive a third party or which advocates or promotes any unlawful act.

vii. Creation, accessing of Unlawful material, or material that is defamatory, threatening, discriminatory, extremist or which has the potential to radicalise themselves or others.

viii. Unsolicited or bulk email (spam), forge addresses, or use mailing lists other than for legitimate purposes related to College’s activities.

ix. Material that brings the College into disrepute.

x. Intentionally bypassing, damaging or disrupting the College's information systems and networks, or interfering with the work of others.

xi. Unauthorised use or disclosure of personal information, confidential information or any other information that is subject to protection under applicable laws or regulations.

xii. Consuming food and drink other than water in any computer room except in the case of College events or by express permission from an authorised person.

xiii. Removal or unplugging, tampering or damaging of IT equipment.

xiv. Misuse of AI tools and services, including but not limited to generating or sharing harmful, misleading, discriminatory, or inappropriate content; using AI to impersonate individuals or fabricate information; bypassing academic integrity policies (e.g., submitting AI-generated work as original student work without disclosure); or deploying AI in ways that compromise data privacy, security, or the College’s reputation. All use of AI must align with the College’s ethical standards, safeguarding policies, and applicable laws.

6. Security and Privacy

6.1. As users of the College's information systems and networks you are responsible for safeguarding your own password, data, and devices. You must take reasonable steps to protect the confidentiality, integrity, and availability of the College's information assets, including:

i. You must use a strong passwords that are at least 8 characters (12 characters for staff) containing capital letters, lower case letters, number and symbols. You must not share your

username and password with anyone else. If you think someone knows your password change it at once or go to the IT Services Department with your ID to have it changed. As a user you are responsible for the security of your accounts and files. Although the College does maintain a backup system, it will not accept any liability whatsoever for loss, damage, or expense which may result from using the College's information systems and networks.

ii. You are not allowed to let anyone else use your account or use anyone else's account yourself. If you do you are breaking the law (Computer Misuse Act 1990).

iii. If you leave a computer unattended make sure you have saved your work and either locked the computer (staff) or logged off (other users).

iv. You may use the College systems whilst you are at NWSLC. Your access and email will be revoked, and your files deleted when you leave the College. Students should make sure when they leave the College to make a backup of your files and emails to take with you.

v. The College may allow users to connect their own personal equipment to the College network via the Eduroam Wireless Network as long as the device has up-to-date software and operating systems with current security patches.

vi. Reporting any suspected security incidents or data breaches to the IT Services Team.

7. Software

7.1. The software you need for your work and study is preinstalled by the College or on supplied media.

i. Under no circumstances are you to try and download or install any software. If you require additional software, please contact the IT Services Department.

ii. You are not to run unauthorised programs from a portable device (such as a memory stick).

iii. The IT Services Team will regularly check network areas and if any unauthorised software is found it will be removed and disciplinary action will be initiated.

8. Monitoring and Enforcement

8.1. The College reserves the right to monitor the use of its information systems and networks for compliance with this policy and for other legitimate purposes, such as ensuring the availability and reliability of its systems, investigating security incidents, and complying with legal obligations. Users should not have any expectation of privacy when using the College's information systems and networks.

8.2. In the case of absence, the College may access your email or workspace for College purposes. In relation to staff, this can only be authorised by two members of the Senior Leadership Team (SLT) or a member of SLT and a manager from the HR Department.

8.3. The College reserves the right to disable access to the network at any time. In relation to staff this can only be approved by a member of the Executive team or by request from HR. The only exception to this is if there is a cybersecurity related incident and any delay would cause damage to the College systems, in this instance the IT team will disable any access immediately.

8.4. Violations of this policy will be investigated and may result in disciplinary action, as determined by the College. In addition, violations may be reported to law enforcement authorities when applicable.

9. Acknowledgement and Agreement

9.1 By accessing or using the College's information systems and networks, users acknowledge that they have read, understood, and agree to abide by this policy. Failure to comply with this policy may result in disciplinary action, up to and including termination of access to the College's information systems and networks.

10. Equality Analysis

10.1 By virtue of the provisions of the Equality Act 2010, the College has a duty to have due regard to the need to:

i. eliminate unlawful discrimination, harassment and victimisation and other prohibited conduct;

ii. advance equality of opportunity between people of different groups;

iii. foster good relations between people from different groups.

10.2 In implementing this Policy and associated procedures, the College will actively take these aims into account as part of its decision making process and will demonstrate how this has been undertaken.

10.3 Where necessary a full equality impact assessment will be undertaken.

11. Data Protection Impact Assessment

11.1 Data Protection Impact Assessments (DPIA) are an essential part of the College's accountability obligations under the UK GDPR. Conducting a DPIA is a legal requirement for any type of processing, including certain specified types of processing that are likely to result in a high risk to the rights and freedoms of individuals. Under UK GDPR, failure to carry out a DPIA when required may leave the College open to enforcement action

11.2 A DPIA, relating to any relevant areas within this Policy and Procedure, will therefore be undertaken to enable the systematic analysis, identification and minimisation of data protection risks and to demonstrate how the College complies with its data protect obligations.

12. Policy Monitoring and Review

12.1 This Policy will be reviewed annually, or as otherwise directed by the Principal, or regulatory / legislative changes.