IT Code of Conduct

Policy number:	AD100	**Policy Owner:**	IT Manager
EIA Status:	Compliant	**EIA meeting date:**	17/07/2025
Approved by:	SLT	**Date approved:**	November 2024
	Committee		
	Board		November 2024
Review frequency:	Tri-Annually	**Next review due:**	01/11/2027
External website:	Yes	**Status:**	Active
Linked policies/ documents			

Policy Summary

Newbury College's IT Code of Conduct outlines rules for responsible use of its IT resources to ensure a secure, respectful, and legally compliant environment for all users. It applies to staff, students, and others using any college IT facilities.

IT Code of Conduct

1. Policy Statement and Purpose

The IT Code of Conduct establishes guidelines for the responsible use of Newbury College's IT facilities.

Purpose

It is designed to ensure compliance with legal requirements and to foster a respectful, secure, and productive computing environment.

Scope

This policy applies to all staff, students, and others using IT facilities at Newbury College, including all types of IT facilities such as PCs, laptops, digital devices, network facilities, remote access, internet, email, printers, and all hardware and software.

2. Responsibilities

Users: All users must adhere to current legislation and all aspects of this Code of Conduct.

IT Services Department: Monitor compliance and provide support and guidance.

3. Procedures

Usage Guidelines

- IT facilities are for educational, research, and course-required activities only. Use for Personal gain is prohibited.
- The uses of the IT facilities are, in general, free of charge, though some facilities, such as printing, may require payment if your initial print credit is exceeded.
- At all times, you must take care not to disturb the other users of the classroom.

Internet Use

- Internet access is for educational purposes only.
- All Internet access is monitored on College owned devices and BYOD connected to the College WiFi network on the main site.
- Access to inappropriate/restricted sites and attempts to bypass filters are strictly prohibited.
- Users must not scan the College network, nor initiate DDoS attacks against devices belonging to the College.

• Email Facilities

- College email accounts are for educational and College business use only.
- The use of personal email accounts used on College devices are subject to this Code.

Equipment

- All College-provided devices remain property of Newbury College and may be reclaimed or replaced at any time.

- Do not move or alter IT equipment without IT Services staff permission.
- Equipment should not be unplugged. In particular, unplugging a network connection to plug your personal PC into the network is strictly forbidden.
- Do not cause damage to IT facilities. Charges may apply for damages caused.
- Users must not eat or drink near any IT facilities except for bottles with sealable lids.
- The loan of IT equipment is only permitted with proper authorisation from IT Services and should be return within the time permitted.
- Users must not reserve computing facilities for absent friends/colleagues.
- Any devices or pen drives found, should be handed in to IT Services or Main Reception.

Software

- Copying or modifying licensed software is forbidden without explicit approval.
- The installation or use of unauthorised software on College devices is prohibited.

Content and Data

- It is forbidden to redistribute or transmit any College owned content, including College provided resources and content provided as part of Teams meetings to anyone outside of the organisation without proper authorisation.
- Any incident that may be deemed to be breaking rules of data protection and/or GDPR regulations must be reported to the Data Protection Officer.
- Once a user has left the College, any data held in a college account will be deleted unless required for GDPR purposes.
- Creation or circulation of offensive, defamatory, inappropriate or copyright-infringing material and/or messages is strictly forbidden.
- Pornographic or other offensive material in any form is not allowed.

Security and Conduct

- Keep login details confidential, except when requested by IT Services.
- Users must log off when they complete a session or take a break, as failure to do so leaves the user account open to abuse.
- Introducing harmful programs or files and circumventing security measures is prohibited.
- Do not attempt unauthorised access to restricted College information.
- Respect others' use of IT facilities and avoid disturbing or removing others' work.

Bring Your Own Device (BYOD) and Remote Access

- Personal devices used to access College facilities and services are subject to this Code.
- The College may require access to your device for security reasons, with your consent.

Liability

- Newbury College accepts no responsibility for the loss of any data, settings, or software that may occur while accessing College facilities or services, during repairs or upgrades.

Reporting incidents

- Report any radicalisation concerns or data protection breaches following the College Safeguarding Procedures.
- Report any misuse of the IT facilities or damage equipment to a member of the IT Services team.

4. Compliance and Enforcement

Users who fail to adhere to this Code may face restrictions on IT use, disciplinary action, and, where applicable, legal consequences.

Anyone found to be breaking the terms of the IT Code of Conduct while using College-provided devices will have them confiscated and will be subject to the College's disciplinary procedure.

Monitoring of IT use is conducted by IT Services to ensure compliance.

5. References

- Data Protection Act 2018
- Communications Act 2003
- Copyright, Designs & Patents Act 1988
- Computer Misuse Act 1990
- Protection from Harassment Act 1997
- Data Protection Act 2018

6. Review and Monitoring

This policy will be reviewed every three years to ensure its effectiveness and compliance with relevant legislation.

Reviewed: Aug 2013, Jan 2016, Aug 16 (minor update), Aug 18 (minor update), Oct 19 (minor update) Nov 23 (minor update), November 2024

Next review date due: November 2026