Exeter College Acceptable Use Policy

1. Purpose

This Acceptable Use Policy (AUP) details the acceptable and unacceptable use of Exeter College IT resources by the College members. It makes clear what the members may or may not do using College equipment, networks or services.

As members of the University and JiSC, the College is bound to the regulations of these organisations. This AUP consolidates all the 'Acceptable Use' elements of these organisations' regulations into a single policy, but it does not replace the full regulations. The full regulations can be viewed at https://community.jisc.ac.uk/library/acceptable-use-policy and http://www.admin.ox.ac.uk/statutes/regulations/196-052.shtml.

2. Scope

The following people and devices fall within the scope of this policy:

- All members using the College owned equipment, using or accessing College or University services or networks for College or personal use
- All members using personal devices on College or University networks, or using College or University services

The following people or devices are out of the scope of this policy:

- Members using personal devices on non-College networks.

3. Acceptable Use

A member of the College may use the IT facilities for:

a) Performing the duties of their role
b) To support teaching, learning or research activities
c) Reasonable private use as long as it does not breach the Acceptable Use Policy, including but not limited to streaming of media content from legal sources
d) Any College equipment must be treated with all due care and attention and kept securely
e) Users must comply with the Counter Terrorism and Security Act 2015

4. Unacceptable use

A member of the College must not use the IT facilities for:

a) Any unlawful activity
b) Creation, storage, downloading, transmission or display of any offensive, obscene or indecent or menacing images, videos or other material
c) Intent to draw people into terrorism
d) Attempt to gain access to any system or network they have not been given access to, or attempt to disrupt or impair any service

e) Creation, storage, downloading, transmission or display of any material to harass another individual.
f) Creation, storage, downloading, transmission or display of any of any material to defame any individual or organisation
g) Downloading, creation or transmission of any material with a view to infringe any copyright, trademark or other intellectual property
h) Send emails that do not correctly identify the true sender or device of origination
i) Send emails to a large groups of users without any consent of the recipients
j) Private profit or commercial purposes except as authorised under your contract of employment or with College approval
k) Deliberate or reckless activities that may result in
    - Wasting staff effort or resources
    - Disruption or corruption of others users data
    - Violating the privacy or work of other users
l) Use of distributed file sharing such as but not limited to BitTorrent, Kazza, eMule, unless it is for legitimate academic purposes.
m) Behaviour constituting a breach of UK or EU data protection or cyber security legislation, including but not limited to the EU General Data Protection Regulation, the Data Protection Act 2018, the Computer Misuse Act 1990 and relevant secondary legislation.

If legitimate research is required which may break any of the above restrictions, then a request should be made in writing to the IT Manager who will review the request and make a decision which will be logged.

5. Enforcement

Breaches in the AUP should be reported to the IT Manager**.**

Failure to comply with the acceptable use policy may result in

- Access to University or College systems being disabled
- Fines for copyright infringement
- Disciplinary action for wilful and serious breaches
- Users being reported to the police and/or appropriate regulatory authorities

6. Responsibilities

The following bodies and individuals have specific information security responsibilities:

- **The Rector** is accountable for the effective implementation of this policy, and supporting information security rules and standards, within Exeter College
- **Governing Body** has executive responsibility for information security within **Exeter College.** Specifically, Governing Body has responsibility for overseeing the management of the security risks to **Exeter College** staff and students, its infrastructure and its information.
- **Users** are responsible for following the AUP and reporting anyone else not following the AUP

Document Control

Date Approved	16th May 2018
Last Review Date	15th June 2022
Policy Owner	IT Manager

Version History

1.2	Approved by Governing Body	16th May 2018
1.3	Amended for GDPR	04th June 2019
	Reviewed unchanged	15th June 2022

By College Order 22/070, this policy was approved by Governing Body on 15th June 2022 with immediate effect, and is to be reviewed by 30th June 2026, and was also approved for display on the website.