NORWICH
UNIVERSITY
OF THE ARTS

Vice-Chancellor: Professor Simon Ofield-Kerr

IT ACCEPTABLE USE POLICY

Pro Vice-Chancellor (Student Experience)

Approved: Version 9 – 4 April 2022

Next Review: May 2023

Contents

1 Introduction

The IT Acceptable Use Policy (AUP) applies to anyone using the IT facilities including:

- Computers, printers, scanners and other peripherals
- Applications, software, file storage
- Cloud based services, email and networks
- Telecommunications include mobile and desktop phones, voicemail etc

It is also applicable to the use of the Joint Academic Network (JANET) through which NUA connects to the Internet and NUA's Wi-Fi network including the use of eduroam.

The aim of this policy is to help ensure that the University's IT (Information and facilities) can be used safely, lawfully and equitably.

It applies to everyone using NUA's IT Services (users) and this includes:

- staff and students using either personal or NUA provided equipment which is connected locally or remotely to NUA's networks
- Visitors using NUA's IT Services
- Students and visitors from other organisations logging onto eduroam

This Acceptable Use Policy (AUP) is to inform users of their responsibilities for the protection of NUA's information, IT systems and their own devices and to provide guidance which helps to mitigate against cyber-attack, malware and other security risks.

2 Authorisation

This policy is issued under the authority of the Senate. The Deputy Vice-Chancellor is responsible for their interpretation and enforcement and may also delegate such authority to other people.

You must not use the IT facilities without due authority. This is usually granted through the issuance of a user ID and password or other IT credentials.

You must comply with any reasonable written or verbal instructions issued by people with delegated authority in support of these regulations. If you feel that any such instructions are unreasonable or are not in support of this policy, you may appeal to the Deputy Vice-Chancellor or through the University complaints procedures.

3 Intended Use

IT facilities are provided for academic and professional use, for example to support a course of study, research or in connection with your employment at NUA. Use of these facilities for personal activities (provided that it does not infringe any of the regulations and does not interfere with others' valid use) is permitted, but this is a privilege that may be withdrawn at any point.

Use of these IT facilities for non-institutional commercial purposes, or for personal gain, requires the explicit approval of the Deputy Vice-Chancellor.

4 Identity

You must take all reasonable precautions to safeguard any IT credentials (for example, a user ID and password, email address, identity card or other identity hardware) issued to you. You must not allow anyone else to use your IT credentials. Nobody has the authority to ask you for your password and you must not disclose it to anyone.

You must not attempt to obtain or use anyone else's credentials.

You must not impersonate someone else or otherwise disguise your identity when using the IT facilities.

5 Infrastructure

The IT infrastructure is all the underlying hardware and software that makes IT function. You must not do anything to jeopardise the integrity of the IT infrastructure by, for example, doing any of the following without approval:

- Damaging, reconfiguring or moving equipment;
- Loading software on the University's IT facilities
- Reconfiguring or connecting equipment to the network other than by approved methods;
- Setting up servers or services on the network;
- Deliberately or recklessly introducing malware;
- Attempting to disrupt or circumvent IT security measures.
- Attempting to impair the operation of University or external IT facilities through, for example, a denial of service attack.

6 Good Practice – the Dos and Don'ts

Dos	Don'ts
Report as soon as possible any loss, theft or damage to any NUA owned IT equipment	Don't share your NUA password with anyone
Do ensure that you look after your own data	Don't install, use or distribute software on NUA owned devices unless it is legally entitled to use the software for NUA purposes.
Do take care when using removable data storage devices or cloud based Google Apps or Dropbox.	Don't send emails that could cause offence to others
Do make use of NUA's OneDrive account that is part of Microsoft 365	Don't connect unauthorised equipment to the NUA network
Do comply with copyright laws	Don't publicly disclose, in anyway, information about the security measures that are used to protect NUA's information and systems.
	Don't access material that is illegal or could pose a security risk to NUA.

7 Information

If you handle personal, confidential or sensitive information, you must take all reasonable steps to safeguard it and must observe NUA's Data Protection policy available at www.nua.ac.uk particularly with regard to removable media, mobile and privately owned devices. Furthermore, use of University equipment off campus, including limited personal use, must be approved.

You must also observe the University's Information Security policy and associated appendices, available at www.nua.ac.uk.

You must not infringe copyright, or break the terms of licences for software or other material.

You must not attempt to access, delete, modify or disclose information belonging to other people without their permission, or explicit approval from the University.

You must not create, download, store or transmit unlawful material, or material that isindecent, offensive, defamatory, threatening, discriminatory or extremist without the explicit approval from the University. The University has procedures to approve and manage valid activities involving such material.

8 Behaviour

The Internet is provided for academic and professional use. The University recognises that many employees and students use the internet for personal purposes and that many participate in social networking on websites. The principle to follow is "do not do anything on line that you would not do off-line".

Whilst recognizing the need to safeguard academic freedom, you must not cause offence to others. All forms of cyber-bullying will be investigated and addressed as a disciplinary matter if upheld.

You must not send spam (unsolicited bulk email).

9 Private Monitoring

The University monitors and records the use of its IT facilities for the purposes of:

- The effective and efficient planning and operation of the IT facilities and the University;
- Detection and prevention of infringement of University regulations;
- Investigation of alleged misconduct;

The University will comply with lawful requests for information from government and law enforcement agencies, as required by legislation mentioned in point 2 (Compliance).

You must not attempt to monitor the use of the IT facilities without explicit authority from the University.

10 Infringement

Infringing this policy may result in the withdrawal of services or sanctions under the institution's disciplinary processes. Offending material will be taken down.

Remedial action (e.g. ensuring IT equipment is free from malware) and/or training may be required before access to IT facilities is restored.

Information about infringement may be passed to appropriate law enforcement agencies, and any other organisations whose regulations you have breached.

The University reserves the right to recover from you any costs incurred as a result of your infringement.

You must inform the University if you become aware of any infringement of this policy.

11 Disclaimers

The University accepts no responsibility for the malfunctioning of any equipment or software, failure in security or integrity of any stored program or data or for any loss alleged to have been caused whether by defect in the resources or by act or neglect of the University, its employees or agents.

Student files and access will be removed once they have completed their course. Students are advised to keep copies or backups of their files on removable media. The University is not liable for the non-retention of this material. Workstations may be wiped and the operating system re--installed at any time.

12 Compliance

It is expected that your conduct is lawful. Ignorance of the law is not a defence for unlawful conduct. You are bound by the University's general regulations when using the IT facilities, available at www.nua.ac.uk.

When accessing services located in a different country than that where you reside, you must abide by the local laws of the country where you reside, as well as the laws applicable in any country where the service or part of it is located.

You must abide by the terms and conditions of use published by any other organisation whose services you access such as Janet, Eduserv and Jisc Services. Software licences procured by the University will set out terms and conditions for the user.

When using services via eduroam (the world-wide roaming access service for international research and education institutions), you are subject to both the regulations of this University and the institution where you are accessing services.

Breach of any applicable law or third party terms and conditions of use will be regarded as a breach of these IT regulations.

The use of computing facilities is subject to provisions of current UK legislation including:

- Obscene Publications Act 1959 and 1964

- Protection of Children Act 1978
- Police and Criminal Evidence Act 1984
- Copyright, Designs and Patents Act 1988
- Criminal Justice and Immigration Act 2008
- Computer Misuse Act 1990
- Human Rights Act 1998
- Data Protection Act 1998
- Regulation of Investigatory Powers Act 2000
- Prevention of Terrorism Act 2005
- Terrorism Act 2006
- Police and Justice Act 2006
- Freedom of Information Act 2000
- Freedom of Information (Scotland) Act 2002
- Equality Act 2010
- Privacy and Electronic Communications (EC Directive) Regulations 2003(as amended)
- Defamation Act 1996 and 2013
- Counter-Terrorism and Security Act 2015
- General Data Protection Act 2018

1	**Name of Document:**	Acceptable Use Policy
2	**Originator:**	Deputy Principal (Finance & Resources)
3	**Date of Origination: Version 1**	8th February 2005
4	**Academic Board Ratification:**	8th February 2005
5	**Assigned Ref Number:** **(by SMT Support)**	SD/P/012
6	**Revision History**	
	Revision 1 **Academic Board Ratification:** **Assigned Ref Number:**	23rd October 2007 Chair's Action 23rd October 2007 SDP004
	Revision 2 **Academic Board Ratification:** **Assigned Ref Number**	4th September 2008 University College Updates 4th September 2008 SDP012
	Revision 3 **Academic Board Ratification** **Assigned Ref Number:**	1st January 2009 New Principal updates SDP012P
	Revision 4 **Academic Board Ratification** **Assigned Ref Number:**	Formatting in accordance with College typography Chairs Action – October 2009 SD/P/012d
	Revision 5 **Academic Board Ratification** **Assigned Ref**	9 August 2010 Change to ownership from DIR Chairs Action 9 August 2010 SD/P/012e
	Revision 6 **Senate Ratification** **Assigned Ref Number:**	April 2013 University updates 6 March 2013 SD/P/12e--U1
	Revision 7 **Ratification** **Assigned Ref Number:**	January 2015 Reviewed by SMT and updated 4 March 2015 SDP012--U2
	Revision 8 **Ratification** **Assigned Ref Number:**	June 2021 Reviewed by SMT and updated SDP012-U3
	Revision 9 **Ratification** **Assigned Ref Number:**	March 2022 Reviewed by Pro Vice-Chancellor (Student Experience) and updated. Approved PVC(SE) 4 April 2022 SDP012-U4