IT Acceptable Use Policy

Organisation	National Film and Television School
Title	IT Acceptable Use Policy
Creator	Head Of Systems/IT
Approvals Required	1. Head of IT 2. Management Team
Version	Version 1.3
Owner	Head Of It
Subject	The IT Acceptable Use Policy of the NFTS
Rights	Public
Review date and responsibility	Annually by Head of IT

Revision History		
v0.1	Draft Acceptable Use Policy	Feb 2017
V0.2	Following management feedback	May 2017
v1.0	Finalising policy following Management Team meeting	June 2017
V1.1	GDPR and staffing updates	August 2018
V1.2	Annual review	November 2020
V1.3	Annual review	February 2023

1. Introduction and Policy Objectives

1.1 Information is an asset of the National Film and Television School (NFTS), and as such, must be protected against unauthorised, accidental or intentional disclosure.

1.2 Computer systems, networks and allied hardware and other peripherals are an integral part of our operations and represent substantial investment.

1.3 The aim of this policy is to ensure the confidentiality, integrity and availability of NFTS information assets by:

- protecting the investment in IT infrastructure
- safeguarding the information and materials contained within these systems ● reducing legal risk
- reducing business risk
- help ensure compliance with data protection legislation including the Data Protection Act 2018 and the GDPR
- preserving the reputation of NFTS
- providing NFTS staff and students (herewith "users") with a safe and acceptable working environment.

1.4 This and other information security policies are not intended to obstruct and limit the use of information at NFTS but to safeguard individuals and the School as a whole against possible risks.

1.5 Please note that infringement of these guidelines may constitute a criminal offence or be a disciplinary offence under Staff Conditions of Service.

2. Access to Staff-Only Information Systems

2.1 Access to NFTS staff-only information systems shall be restricted. Each user shall be granted initial data access as determined by their line manager. Additional access, as required by users on a case by case basis, will be applied in accordance with the School's IT Access Control Policy

3. Student Use of IT Facilities

3.1 Changes to hardware and software should only be made by authorised members of NFTS staff.

3.2 Please respect the legitimate use by others of the IT facilities and do not remove or interfere with output belonging to others.

3.3 IT facilities are primarily provided for academic reasons and not for the purposes of entertainment.

3.4 Please respect the rights of others and should conduct yourself in a quiet and orderly manner when using IT facilities.

4. Electronic Information, online access and email

4.1 NFTS provides its users with computer equipment, software and online access to internal and external networks and network services, including the Internet. This provision is so that users may communicate more efficiently and better accomplish the School's aims.

4.2 Although NFTS respects the privacy of its users, you should have no expectation of privacy. Furthermore, you should be aware that (generally) any emails, computer files and/or documents you create are the property of NFTS.

4.3 Access to another person's emails will only be granted with the explicit consent of two of the following NFTS managers: Director, Head of IT, Director of HR, Director Of External Relations, Director of Curriculum, Registrar.

4.4 Use of computer equipment, software or online access provided by NFTS is subject to the following general conditions:

- As a general rule, your use of IT equipment and online access should be for academic or work purposes only. However, NFTS does allow personal use of email and the internet subject to the rules of conduct set out in this policy and provided that such use does not conflict with the performance of your duties or the interests of NFTS.
- You must not reveal your account password (or associated secret authentication information) to others or allow use of your account by others. This includes family

and other household members when working from home and deputies when you are away from work.

- You must not use the NFTS's IT or network facilities for anything listed in the table, below.

Prohibited use
Gaining unauthorised access to, or intentionally damaging, other computer systems, network services or the information contained within them
Any unlawful activity (including infringing a trademark, copyright or any other intellectual property right; breaching another person's rights of privacy; and sending unsolicited advertising or promotional material
Viewing, distributing or obtaining illegally copied software, media or other material
The creation, transmission, storage, downloading or display of any offensive, obscene, discriminatory (either on the grounds of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion of belief, sex or sexual orientation), indecent or threatening data or other material (unless such access is necessary as part of authorised research activities)
The creation or transmission of defamatory or libellous material about any individual or organization
Private profit, except to the extent authorised under your conditions of employment or other agreement with NFTS
The transmission of unsolicited commercial or advertising material
Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by NFTS
Unauthorised copying of copyrighted material including, but not limited to, digitisation and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which NFTS or the end user does not have an active license is strictly prohibited
Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs etc).
Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorised to access. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes

Port scanning or security scanning is expressly prohibited unless being conducted by authorised members of NFTS IT Team (or authorised third parties) for the purposes of maintaining the integrity of NFTS network security
Executing any form of network monitoring that will intercept data not intended for the user's host is expressly prohibited unless being conducted by authorised members of NFTS IT Team (or authorised third parties) for the purposes of maintaining the integrity of the NFTS network or its security
Circumventing user authentication or security of any host, network service or account
Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's network session, via any means, locally or via the Internet/Intranet/Extranet
Providing information about, or lists of, NFTS staff or students to parties outside of NFTS (unless authorised by senior management)

4.5 No confidential information will be stored on any systems other than those directly maintained by NFTS unless formally approved by the NFTS Head of IT.

4.6 No confidential information should be sent online by any means, without utilising appropriate, approved, security methods. Online communications may be subject to interception by persons outside NFTS and such interception may not be detectable. Any encryption software used should be provided by or approved by the NFTS IT Team.

4.7 NFTS will cooperate with law enforcement authorities to prosecute offenders. You must report any suspected, accidental, or intentional illegal action to the Head of IT or Director or Operations.

4.8 NFTS has the right to monitor all usage of the IT, communications and computer systems to:

- ensure proper working of the systems
- ensure that all users comply with NFTS practices and procedures (including but not limited to this policy)
- ensure that all users achieve acceptable standards in relation to the performance of their duties and observance of this policy

- prevent or detect crime, and/or
- investigate or detect the unauthorised use of NFTS's systems.

4.9 NFTS reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.10 NFTS may inspect all such computers and information at any time as is deemed necessary for the conduct of its business, or for reasons of security at its sole discretion.

4.11 Users must adhere to the terms and conditions of all licence agreements relating to IT facilities which you use including software, equipment, services, documentation and other goods. You are deemed to have agreed to the Copyright Acknowledgement for the appropriate supplier – see appendix

5. Automatically Forwarded Email

5.1 Automatic email forwarding may potentially result in the inadvertent transmission of sensitive information to external email accounts.

5.2 Users should exercise utmost caution when sending any email from their NFTS account to an outside network. Unless approved by an appropriate manager, NFTS email should not be automatically forwarded to an external destination.

6. Prevent Duty

6.1 Under Section 26 of the Counter-Terrorism and Security Act 2015, the School has a statutory duty to have 'due regard to the need to prevent people from being drawn into terrorism.' One aspect of this covers the accessing of online material that is proscribed under anti-terrorism legislation. Students should be aware that downloading or transmitting extremism-related material may present serious legal risks, and place them in danger of arrest and prosecution by the authorities.

6.2 In instances where students consider that they need to access security-sensitive material for legitimate purposes of academic research, they should request this in writing from the Director of Curriculum and Registrar, and suitable arrangements shall be made.

Appendix 1

Software	Agreement
Microsoft	https://www.microsoft.com/online/mosa/MOSA2014Agr(NA)(ENG)(Nov2014)(HTML).htm
The Foundry	https://www.thefoundry.co.uk/EULA/EULA.pdf
Maxon	http://www.maxon.net/fileadmin/MAXON_Content/100_Administrative/30_Legal/MAXON_EULA_2015_EN.pdf
Entertainment Partners	https://www.ep.com/eula/
	https://www.finaldraft.com/company/legal/eula
Filemaker	https://www.filemaker.com/company/legal/docs/eula/fmpa_eula_wwe.pdf
Papercut	https://www.papercut.com/products/ng/manual/common/topics/license.html
Manageenging	https://www.manageengine.com/eula.html
Avid	http://www.avid.com/legal/end-user-license-termsfor-avid-software
Adobe	http://www.eduserv.org.uk/codeofconduct.aspx http://www.adobe.com/legal/terms/enterpriselicensing.html
Veeam	https://www.veeam.com/eula.html