Information Security Policy

Organisation	National Film and Television School
Title	Information Security Policy
Creator	Director of Operations
Approvals Required	1. Head of IT 2. Director of Operations 3. Management Team
Version	1
Owner	Director of Operations
Subject	The formal approved information security policy of NFTS
Rights	Public
Review date and responsibility	Annually by Head of IT/Director of Operations

Revision History		
v0.1	Draft Information Security Policy	Feb 2017
V0.2	Incorporating management feedback	March 2017
V.0.3	Incorporating further management feedback re alignment with data protection policy	March 2017
v1.0	Finalising policy following Management Team meeting 4/4/17	April 2017

1. Introduction

NFTS recognises that information and the associated processes, systems and networks are valuable assets and that the management of personal data has important implications for individuals. Through its security policies, procedures and structures, the School will facilitate the secure and uninterrupted flow of information, both within the School and in external communications. The School believes that security is an integral part of the information sharing which is essential to academic and corporate endeavour and this Policy is intended to support information security measures throughout the School.

2. Definition

2.1 For the purposes of this document, information security is defined as the preservation of:

- confidentiality: protecting information from unauthorised access and disclosure;
- integrity: safeguarding the accuracy and completeness of information and processing methods;
- availability: ensuring that information and associated services are available to authorised users when required.

2.2 Information exists in many forms. It may be printed or written on paper, stored electronically, transmitted by post or using electronic means, shown on films, or spoken in conversation. Appropriate protection is required for all forms of information to ensure business continuity and to avoid breaches of the law and statutory, regulatory or contractual obligations.

3. Protection of Personal Data

The School holds and processes information about employees, workers, freelancers, students, and other data subjects for academic, administrative and commercial purposes. When handling such information, the School, and all staff or others who process or use any personal information, must comply with the Data Protection Principles which are set out in the Data Protection Act 1998 (the 1998 Act) and the School's Data Protection policy.

4. Information Security Responsibilities

4.1 The School believes that information security is the responsibility of all students and members of staff. Every person handling information or using School information systems is expected to observe the information security policies and procedures, both during and, where appropriate, after his or her time at the School.

4.2 This Policy is the responsibility of the Management Team; supervision of the Policy will

be undertaken by the Director of Operations. This policy may be supplemented by more detailed interpretation for specific sites, systems and services. Implementation of information security policy is managed through the Head of IT and IT team, which reports to the Director of Operations.

4.3 The School's IT team has operational responsibility for the School's IT systems and will therefore take action wherever necessary to protect those systems. Regular penetration testing will be undertake.

5. Information Security Education and Training

The School recognises the need for all staff, students and other users of School systems to be aware of information security threats and concerns, and to be equipped to support School security policy in the course of their normal work.

6. Compliance with Legal and Contractual Requirements

6.1 Authorised Use: School IT facilities must only be used for authorised purposes. The School may from time to time monitor or investigate usage of IT facilities; and any person found using IT facilities or systems for unauthorised purposes, or without authorised access, may be subject to disciplinary, and where appropriate, legal proceedings. Further details are included in the School's IT Acceptable Use Policy.

6.2 Monitoring of Operational Logs: The School shall only permit the inspection and monitoring of operational logs by the appropriate staff from the School's IT team or where it has been otherwise authorised. Disclosure of information from such logs, to officers of the law or to support disciplinary proceedings, shall only occur (i) when required by or consistent with law; (ii) when there is reason to believe that a violation of law or of a School policy has taken place; or (iii) when there are compelling circumstances (circumstances where failure to act may result in significant bodily harm, significant property loss or damage, loss of significant evidence of one or more violations of law or of School policies).

6.3 Access to School Records: In general, the privacy of users' files will be respected but the School reserves the right to examine systems, directories, files and their contents, to ensure compliance with the law and with School policies and regulations, and to determine which records are essential for the School to function administratively or to meet its teaching obligations. Except in emergency circumstances, authorisation for access must be obtained from at least two of the following: Head of IT, Director of Operations, Director of HR, Deputy Director, one of whom would normally be the Director of HR or the Deputy Director. It shall be limited to the least perusal of contents and the least action necessary to resolve the situation.

6.4 Protection of Software: To ensure that all software and licensed products used within the School comply with the Copyright, Designs and Patents Act 1988 and subsequent Acts, the School may carry out checks from time to time to ensure that only authorised products are being used. Unauthorised copying of software or use of unauthorised products by staff or students may be grounds for disciplinary, and where appropriate, legal proceedings.

6.5 Virus Control: The School will maintain detection and prevention controls to protect against malicious software and unauthorised external access to networks and systems. All users of electronic devices issued by the School or used for School business shall comply with best practice, as determined from time to time by the School's IT team, in order to ensure that up-to-date virus protection is maintained.

7. Asset Management

All School information assets (data, software, computer and communications equipment) shall be accounted for and have a designated owner. The owner shall be responsible for the maintenance and the protection of the assets concerned.

8. Physical and Environmental Security

Physical security and environmental conditions must be commensurate with the risks to the area concerned. In particular, critical or sensitive information processing facilities must be housed in secure areas protected by defined security perimeters with appropriate security barriers and/or entry controls.

9. Information Systems Acquisition, Development and Maintenance

9.1 Information security risks must be identified at the earliest stage in the development of business requirements for new information systems or enhancements to existing information systems.

9.2 Controls to mitigate the risks must be identified and implemented where appropriate.

10. Access Control

10.1 Access to information and information systems must be driven by business requirements and be commensurate and proportionate to the business need.

10.2 A formal access control procedure shall be required for access to all information systems and services.

11. Communications and Operations Management

Responsibilities and procedures for the management, operation and ongoing security and availability of all data and information processing facilities must be established.

12. Retention and Disposal of Information

All staff have a responsibility to consider security when disposing of information in the course of their work. Owners of information assets should establish procedures appropriate to the information held and processed and ensure that all staff are aware of those procedures.

13. Reporting

All staff, students and other users should report immediately via Freshdesk*, any observed or suspected security incidents where a breach of the School's security policies has or may have occurred, and any security weaknesses in, or threats to, systems or services.

*https://nfts.freshdesk.com/support/home or by telephone to Reception on 01494 671234

14. Business Continuity

The School will implement, and regularly update, a business continuity management process to counteract interruptions to normal School activity and to protect critical processes from the effects of failures or damage to vital services or facilities.

15. Password Policy

15.1 Password Creation

15.1.1 All user-level and system-level passwords must conform to current best practice guidelines (so called, 'strong' passwords). For further information please contact the IT team, however in general 'strong' passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g. 0-9, -_.!~*()
- Are at least ten alphanumeric characters long
- Are not based on personal information, names of family, etc.

15.1.2 Users must not use the same password for NFTS accounts as they do for personal / non-NFTS accounts.

15.1.3 Where possible, users must not use the same password for different accounts.

15.1.4 User accounts that have system-level privileges granted through group memberships, or programs such as Sudo, must have a different password from all other accounts held by that user to access system-level privileges.

15.2 Password Change

15.2.1 Users must abide by local or application-specific guidelines on the frequency of password changes. Changing passwords in itself is not a guarantee of security.

15.3 Password Protection

15.3.1 Passwords must not be shared with anyone (including other NFTS staff). All passwords are to be treated as sensitive and confidential NFTS information.

15.3.2 Do not write passwords down and store them in your office or place of work. Do not store passwords in a computer file unless the file itself is encrypted.

15.3.3 The use of 'remember my password' in applications (e.g. browsers) is not recommended for NFTS passwords.

15.3.4 Any user that suspects their password may have been compromised must change it and inform the IT team immediately.

15.3.5 The use of password manager (also known as password vault) applications is permitted. For further information please contact the IT team.

15.4 Multi-Factor Authentication

15.4.1 It is recommended that users enable multi-factor authentication functionality on all system accounts where available