IT Monitoring Policy

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

Revision History		
V0.1	Draft Monitoring Policy	Feb 2017
V0.2	Following management feedback	May 2017
V1.0	Finalised policy	June 2017
V1.1	GDPR and staffing updates	August 2018
V1.3	Annual review	March 2023

1. Introduction

School communication networks and IT systems are monitored, to ensure their smooth operation and security. Staff engaged in monitoring must be properly authorised.

It is important to be aware of the distinction made between:

- intercepting information in transit - email messages being sent, for example, or watching the web pages visited - here the relevant law is found in the Regulation of Investigatory Powers Act 2000 (RIPA) and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (LBPR);
- examination of material stored on a computer - the law applicable here may vary according to variables such as who owns the computer, what material is being examined, and how the material is examined. However, the Human Rights Act 1998 and the Data Protection Act 1998 provide an over-arching framework to protect the individual's right to privacy

Under the Regulation of Investigatory Powers Act 2000, unlawful interception of communications on the School's computer network may lead to criminal proceedings against an individual operating without the School's authority; unlawful interception may also lead to civil action against the institution where the institution authorized the interception. The RIPA and LBPR do, however, allow for legitimate interceptions of communications by organisations on their private computer and telecommunications networks - in other words, they provide 'lawful authority'.

Systems are also monitored to ensure the following benefits:

1. Minimise downtime
   Quickly identify the causes of issues and therefore minimise downtime.

2. Improve incident response
   Quickly identify the causes of incidents and therefore enable appropriate action to be taken with minimal delay, thereby reducing any potential damage to the organisation or its data/services.

3. Reduce the risk of future issues
   Teams can identify potential abnormalities before breach/downtime occurs then work to mitigate them, moving from a reactive to proactive service.

4. Improve the user experience
   Improve the experience for all users, because applications and systems are available and running at peak performance with less interruption.

2. Scope

All servers, workstations, mobile devices and other IT systems either owned by the School, connected to the School's networks or located on School premises. This includes School-owned machines used at home and personal systems that are connected to the School's networks (including wireless).

This policy also applies to any partner organisations connected to the School's networks, and such connections will monitored for compliance with the terms of their agreement and the JANET acceptable use policy.

3 Important Information for Users

3.1 General

Users are informed that their use of the School's data communications infrastructure, IT services, systems and applications may be monitored by authorised staff as permitted by UK legislation and in accordance with this policy. Further details of what is monitored is in Annex (A).

The School reserves the right to examine any file residing on any system within the scope of this policy. As a condition of connection to the School network, system owners must agree that IT Department staff or other authorised staff may inspect their systems on request and at any reasonable times.

The School also performs active scanning of its networks and connected systems – see Annex (A).

It is recognised that, in the course of their work, system administrators and other authorised IT staff will occasionally come across content of files, emails or other communications. Appropriate steps are taken to minimise the likelihood and impact of this.

3.2 Purpose

Monitoring takes place for the following purposes:

- Ensuring the smooth operation of, and safeguarding the security, integrity and availability of the School's data communications network, computer systems and other IT infrastructure
- Fault investigations
- Security incident handling
- Capacity planning for network expansion and service upgrades
- Detecting and investigating unauthorised use
- Compliance checks against School policies and regulatory requirements
- Law enforcement requests

4. Authorised Staff

The Director of the School and the Data Protection Officer have granted the Head of Systems/IT the following delegated authority:

> *To authorise members of their staff to perform Network, Systems, Applications and Data Communications monitoring procedures that conform to this Policy and all relevant UK laws and regulations*.

In appropriate circumstances heads of other areas may obtain delegated authority to authorise appropriate staff to monitor only those service elements for which complete responsibility lies within their area.

It will be considered a disciplinary offence for anyone to engage in monitoring activities without proper authorisation, or to monitor outwith their areas of responsibility. Furthermore, it is likely that any individual who violates this policy will be breaking the law.

5. Ethics and Safeguards

Authorised staff including network and system administrators must execute their duties in accordance with all relevant UK law and all of the School's relevant policies. In particular, authorised staff must:

- Respect the privacy of others, at all times
- Not use or disclose information realised in the monitoring process for purposes other than those for which the process was approved
- Safeguard information collected in the monitoring process against any potential unauthorised access
- Destroy information collected in the monitoring process in accordance with the appropriate retention schedule.

Annex A - What is Monitored

IT Services, Systems and Applications

All systems providing network services or applications may be monitored for:

- CPU utilisation Active processes
- Filestore - utilisation, anomalies, file types and file sizes
- Licensed software compliance
- Network statistics e.g. peak and average bandwidth utilisation and errors
- System and security log anomalies
- Successful and unsuccessful access attempts - user account, remote IP address, date/time stamp, session duration
- Unusual network traffic

Details of logs kept by certain specific central IT systems are below. Note – this is not an exhaustive list.

Email

The School email systems keep logs of message delivery including:

Timestamp, sender+recipient email address & mail server IP address, message size, message-id

Web Access

Web access is logged, including access to and from external sites, for the following purposes:

- Investigating cases of suspected unauthorised use or illegal activity that are reported
- Investigating cyber security incidents
- Compromised host identification

The information logged includes:

Timestamp, client+server IP address, URL, User-Agent, Referrer

Intrusion Detection Systems

The School operates Intrusion Detection Systems (IDS) that look for recognisable signatures of attack profiles. This is to identify malicious activity, including cyber attacks and compromised hosts. When a signature is recognised an event is logged including:

Timestamp, source/destination IP address/port, signature-id, suspect payload

Network Monitoring

School networks are monitored for protocols and applications in use, sources and destinations (traffic patterns), performance metrics, volume sent/received per router and switch interface, and failure conditions.

Also, logs of network traffic are kept on a “per-flow” basis, including:
Timestamp, Source + destination IP addresses, TCP/UDP port numbers, volume

Under exceptional circumstances e.g. to help investigate incidents or fault conditions, the full content of specific interactions between endpoints may be recorded for analysis. Records are retained for as long as the issue is active, after which time the information is destroyed.

Data communications infrastructure records and associations

Detailed records and inventories are maintained for all components of the data communications infrastructure including fibre optic cabling systems, building premises distribution schemes, backbone and edge routers and switches.

Associations are recorded between specific network connection points, MAC addresses, IP addresses and DNS names, and changes are tracked.

Active scanning

Authorised staff may perform active scanning of systems, applications and network segments to identify vulnerabilities or non-compliance with other School policies. Authorised staff must exercise due diligence, in particular:

- Inform the network and systems administrators responsible for the systems on a segment of the planned scan activity and provide the following:
  - Schedules including Time and duration of scans
  - Systems performing the scan, (IP addresses)
  - Object of the scan i.e., vulnerabilities to be tested
- Take reasonable steps to ensure the continued operation or functionality of systems being scanned
- Identify systems with vulnerabilities to the relevant system administrators

Users of personal systems should note that active scanning would apply to any personal system connected to the School’s networks. Any user who considers this condition unacceptable should not connect their system to the network.

Further information

For further information, please contact the IT Department.