IT Systems: Acceptable Use Policy

Policy owner:	Northern School of Contemporary Dance: Leadership Team
Lead contact:	IT Systems Manager
Audience:	Students/Staff/partners for Northern School of Contemporary Dance Courses of higher education
Approving body:	Northern School of Contemporary Dance: Senate
Date approved:	February 2025
Policy Implementation date:	February 2025
Supersedes:	E-Safety & Online Policy Acceptable Use Policy
Previous approved version(s) dates:	2021
Review cycle:	3 yearly
Next review due date:	April 2028
Related Statutes, Ordinances, General Regulations	Validating Universities' Academic Regulations Equality Act 2010
Related Policies, Procedures and Guidance:	NSCD Privacy Statements, Recommendations for Safe Use of Social Media, Staff and Student Codes of Practice, Safeguarding & Prevent Policy
UK Quality Code reference:	
OfS Conditions reference:	
Equality and Diversity Considerations:	Policy should be available in accessible format for all students.
Date Equality and Diversity Assessment Completed:	
Further information:	

IT SYSTEMS: ACCEPTABLE USE POLICY 1

1. Introduction 3

2. Scope & Principles 3

3. Definitions 3

4. Use Of It Systems 4
4.1 Computer Access Control – Individual's Responsibility 4
4.2 Internet, Social Media, And Email - Conditions of Use 4
4.3 Clear Desk and Clear Screen Policy 5
4.4. Working Off-Site 5
4.5 Mobile Storage Devices 5
4.6 Confidentiality and Data 5
4.7 Software 6
4.8 Viruses 6
4.9 Actions Upon Termination of Contract 6
4.10 Monitoring and Filtering 6

5. Responsibilities 7

6. Communication of Policy 7

7 Legal Framework 7

8 Breach of the Policy 8

9. Complaints 8

10. Related Documents 8

11. Key contacts 9

IT Systems: Acceptable Use Policy

1. Introduction

1.1 This **IT Systems: Acceptable Use Policy** for IT Systems are designed to protect Northern School of Contemporary Dance (NSCD), our employees, students, and other partners from harm caused by the misuse of our IT systems and data. Misuse includes both deliberate and inadvertent actions.

1.2 The repercussions of misuse can be severe, including malware infection (e.g. computer viruses), legal and financial penalties for data leakage, and lost productivity due to network downtime. All users are responsible for the security of our IT systems and the data on them and must adhere to the guidelines in this policy. Should any user be unclear about the policy or its impact on their role, they should speak to their manager, tutor, or a member of the IT department.

2. Scope & Principles

2.1 The policy applies to all processes relating to activities of NSCD and is applicable to all those who engage with NSCD including governors, students, staff including permanent or temporary contractors and others employed under a contract of service and visitors.

2.2 It applies to all conduct of NSCD including activities outside of NSCD that is related to its activities.

2.3 This universal policy applies to all users and all Systems. Specific policies exist for some users or systems (e.g. students); in such cases, the more specific policy takes precedence where conflicts arise. This policy covers internal use of NSCD's systems and does not address use of our products or services by third parties.

2.4 NSCD reserves the right to monitor and/or block access to unlawful or harmful material. Users who believe they have encountered such material should report it immediately to NSCD's Safeguarding team.

3. Definitions

Users: Anyone who has access to any of NSCD's IT systems, including permanent and temporary employees, contractors, agencies, consultants, suppliers, students, visitors, and business partners.

Systems: All IT equipment that connects to the corporate network or accesses corporate applications, including desktop computers, laptops, smartphones, tablets,

printers, data and voice networks, networked devices, software, electronically stored data, and portable data storage devices.

4. Use Of It Systems

4.1 Computer Access Control – Individual's Responsibility

Access to NSCD's IT systems is controlled using User IDs and passwords. All User IDs and passwords are uniquely assigned, making individuals accountable for all actions on NSCD's IT systems.

Individuals must not:

- Allow anyone else to use their user ID and password.
- Leave their accounts logged in on unattended and unlocked computers.
- Use someone else's user ID and password to access IT systems.
- Leave their password unprotected.
- Attempt unauthorised changes to IT systems or information.
- Access data they are not authorised to use.
- Exceed the limits of their authorisation.
- Connect any non-NSCD authorised device to the corporate network without permission.
- Store NSCD data on non-authorised equipment.
- Transfer NSCD data or software outside NSCD without the authority of senior management or the IT department.

Line managers must ensure individuals are given clear direction on the extent and limits of their authority regarding IT systems and data.

4.2 Internet, Social Media, And Email - Conditions of Use

The use of internet, social media, and email is intended for work use and to aid in studies. Personal use is permitted if it does not affect work/study performance, is not detrimental to NSCD, does not breach any terms and conditions of employment, and does not violate statutory or legal obligations.

All users are accountable for their actions online.

Individuals must not:

- Use the internet, social media, or email for harassment or abuse.
- Promote or encourage extremism or radicalisation.
- Use profanity, obscenities, or derogatory remarks in communications.
- Access, download, send, or receive data considered offensive by NSCD.
- Use the internet or email to gamble.
- Distribute chain letters or spam via email.
- Place any information about NSCD on the internet without authorisation.
- Send unprotected sensitive or confidential information externally.
- Forward confidential internal mail to personal email accounts.

- Make official commitments on behalf of NSCD unless authorised.
- Download copyrighted material without appropriate approval.
- Infringe copyright, database rights, trademarks, or other intellectual property.
- Download software from the internet without prior approval from the IT Department.
- Connect NSCD devices to the internet using non-standard connections.

4.3 Clear Desk and Clear Screen Policy

To reduce the risk of unauthorised access or loss of information, NSCD enforces a clear desk and screen policy:

- Computers must be logged off or locked when left unattended.
- Confidential material must not be left on printers or photocopiers.
- All printed business-related matter must be disposed of using confidential waste bins, bags, or shredders.

4.4. Working Off-Site

Laptops and mobile devices may be taken off-site, subject to the following controls:

- Equipment and media must not be left unattended in public places or visible in cars.
- Laptops should be carried as hand luggage when travelling.
- Information must be protected against loss or compromise when working remotely.
- Remote access is preferred for off-site work, keeping all data secure onsite.
- NSCD laptops are configured for remote access by default.
- Mobile devices must be protected by a password or PIN and, where available, encryption.

4.5 Mobile Storage Devices

Mobile devices such as memory sticks, CDs, DVDs, and removable hard drives should only be used when network connectivity is unavailable or for extra storage capacity (e.g., video files). Remote access is preferred for off-site work. Data should not be taken off-site on mobile storage devices without permission, and it should be securely disposed of. Only NSCD-authorised mobile storage devices with encryption enabled should be used to transfer sensitive or confidential data.

4.6 Confidentiality and Data

NSCD is committed to protecting the privacy of our staff, students, and parents/carers. Members of staff may access confidential information about students and others as part of their duties, including highly sensitive information, which must not be shared

outside NSCD without proper justification (e.g., a risk of harm or an agreed multi-agency plan).

NSCD ensures data is collected, used, and managed correctly. We will keep staff, students, and parents/carers informed about how their data is handled.
Data captured includes attendance, assessment data, registration records, SEND data, and relevant medical information. Through effective data management, we can monitor and evaluate the wellbeing and academic progression of students.

In line with **GDPR 2016** and NSCD's Data Protection Policy, we will follow good practice principles when processing data. Data will be securely processed, kept for the regulated period, and not transferred without adequate protection.

NSCD may be required to pass information to external agencies for legal or safety reasons (e.g., Children's/Adult's Social Work Services), which adhere to GDPR and their own data protection policies.

4.7 Software

Users must use only software authorised by NSCD on its computers. All software must comply with the supplier's licensing agreements and be approved by the IT Manager.
Individuals must not:

- Store personal files (e.g., music, video, photographs, games) on NSCD IT equipment.

4.8 Viruses

The IT department implements automated virus detection and updates. All PCs have antivirus software to detect and remove viruses automatically.
Individuals must not:

- Remove or disable anti-virus software.
- Attempt to remove infected files or clean up an infection using anything other than approved antivirus software and procedures.

4.9 Actions Upon Termination of Contract

All NSCD equipment and data must be returned upon termination of contract. All data or intellectual property developed during employment remains the property of NSCD unless stated otherwise.

4.10 Monitoring and Filtering

All data created and stored on NSCD computers is the property of NSCD, with no official provision for individual data privacy. However, we will avoid opening personal emails when possible.

IT system logging may occur, and investigations will be initiated where reasonable suspicion exists of a policy breach. NSCD reserves the right to monitor activity on its systems, including internet, email, and social media use, to ensure security and effective operation. Monitoring will adhere to the **UK Data Protection Act 1998**, the **Regulation of Investigatory Powers Act 2000**, and the **Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000**.

NSCD employs filtering of web content to ensure appropriate and efficient internet use, fulfilling our obligations under **Prevent**. Examples of content filtering include website categorisation, blacklisting, and whitelisting.

5. Responsibilities

5.1 All members of NSCD have a responsibility to abide by and promote the principles in this policy in relation to their work and duties at NSCD:

- The policy is known, understood, and implemented
- Individual behaviours take into consideration the impact it may have upon others
- Everyone is treated with respect and dignity
- Where a member of staff has concerns, they should raise this with their line manager or other relevant staff.

5.2 The IT Systems Manager is responsible for this policy.

6. Communication of Policy

6.1 This policy will be published in staff and student handbooks, available on public display and posted on the NSCD Virtual Learning Environment and public website.

6.2 NSCD will endeavour to provide documents in different formats if requested by applicants, staff and students.

6.3 The induction of all staff will include specific reference to the policy and the responsibility of staff to reflect its principles in their own practice.

7 Legal Framework

7.1 In accordance with UK law, the use of NSCD's IT infrastructure, systems, and services for any activity that may reasonably be regarded as unlawful is not

permitted. Under the **Counter Terrorism and Security Act 2015**, staff, students, and visitors must not create, download, store, or transmit unlawful material or material that is indecent, offensive, defamatory, threatening, discriminatory, or extremist.

7.2 Staff members monitoring compliance with this policy must ensure they remain compliant with relevant local legislation.

7.3 Applicable laws and policies governing the provision and use of IT facilities include (but are not limited to):

- Regulation of Investigatory Powers Act 2000
- Computer Misuse Act 1990
- Data Protection Act 2018
- General Data Protection Regulations
- Freedom of Information Act 2000
- Copyright, Designs & Patents Act 1988
- Telecommunications Act (1984) and (1988)

8 Breach of the Policy

8.1 Northern School of Contemporary Dance will take seriously any instances of infringement of this policy by students, staff, users or participants.

8.2 Any instances of infringement will be investigated and where appropriate will be considered under the relevant complaints/grievance and disciplinary policy for staff or students.

9. Complaints

9.1 Staff, students or visitors who wish to make a complaint regarding this policy should seek resolution through the complaints procedure if unable to be resolved through informal means.

- Student Complaints Policy & Procedures
- Staff Complaints Policy & Procedures
- Public Complaints Procedure

10. Related Documents

This policy should be read in conjunction with:

- NSCD Safeguarding Policy
- NSCD Prevent Strategy
- Recommendations for Safe use of Social Media

- School Policy on Handling and Storage of Security Sensitive Materials
- Staff & Student Codes of Conduct

11. Key contacts

For any questions regarding this policy, please contact the IT Department or the HR Department.