Northern School of Contemporary Dance

Acceptable Use Policy for IT Systems

Name of Policy Writer	Amendments Date Written & agreed	Amended / Approved by	Review Date
Vinny Davies	July 2015		July 2017
Nick Holland (CDD)	October 2017		September 2019
Glenn Glidden	November 2017		September 2019
Tracy Witney	January 2021		October 2022

ACCEPTABLE USE POLICY FOR IT SYSTEMS

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

The repercussions of misuse of our systems can be severe. Potential damage includes, but is not limited to, malware infection (e.g. computer viruses), legal and financial penalties for data leakage, and lost productivity resulting from network downtime.

Everyone who works or studies at the Northern School of Contemporary Dance is responsible for the security of our IT systems and the data on them. As such, all users must ensure they adhere to the guidelines in this policy at all times. Should any user be unclear on the policy or how it impacts their role they should speak to their manager, tutor or to a member of the IT department.

DEFINITIONS
“NSCD” is an abbreviation of the establishment’s name, the Northern School of Contemporary Dance.

“Users” are everyone who has access to any of NSCD’s IT systems. This includes permanent employees and also temporary employees, contractors, agencies, consultants, suppliers, students, visitors and business partners.

“Systems” means all IT equipment that connects to the corporate network or access corporate applications. This includes, but is not limited to, desktop computers, laptops, smartphones, tablets, printers, data and voice networks, networked devices, software, electronically-stored data, portable data storage devices, third party networking services, telephone handsets, video conferencing systems, and all other sim150ilar items commonly understood to be covered by this term.

SCOPE
This is a universal policy that applies to all Users and all Systems. For some Users and/or some Systems a more specific policy exists (such as for our students): in such cases the more specific policy has precedence in areas where they conflict, but otherwise both policies apply on all other points.

This policy covers only internal use of NSCD’s systems and does not cover use of our products or services by third parties.

Some aspects of this policy affect areas governed by local legislation in certain countries (e.g., employee privacy laws): in such cases the need for local legal compliance has clear precedence over this policy within the bounds of that jurisdiction. In such cases local teams should develop and issue users with a clarification of how the policy applies locally.

In accordance with UK law, the use of NSCD’s IT infrastructure, systems and services for any activity which may reasonably be regarded as unlawful is not permitted. NSCD has a statutory duty, under the Counter Terrorism and Security Act 2015, termed “PREVENT”. Staff, students and visitors using the IT systems must not create, download, store or transmit any unlawful material, or material that is indecent, offensive, defamatory, threatening discriminatory or extremist. NSCD reserves the right to monitor or block access to such material. If a ‘user’ believes they may have encountered such material, they should report this immediately to NSCD’s Safeguarding team.

Staff members at NSCD who monitor and enforce compliance with this policy are responsible for ensuring that they remain compliant with relevant local legislation at all times.

Links to local laws and legislation relating to this document are provided at the end of this document (if you are reading this in an electronic format) or copies can be obtained from the IT department.

USE OF IT SYSTEMS

COMPUTER ACCESS CONTROL – INDIVIDUAL'S RESPONSIBILITY
Access to NSCD's IT systems are controlled by the use of User ID's and passwords.
All User IDs and passwords are uniquely assigned to named individuals and consequently, individuals are accountable for all actions on NSCD's IT systems.

INDIVIDUALS MUST NOT:
- Allow anyone else to use their user ID and password on any IT system.
- Leave their user accounts logged in at an unattended and unlocked computer.
- Use someone else's user ID and password to access IT systems.
- Leave their password unprotected (for example writing it down on a piece of paper).
- Attempt to perform any unauthorised changes to IT systems or information.
- Attempt to access data that they are not authorised to access or use.
- Exceed the limits of their authorisation or specific business need to interrogate the system or data.
- Connect any non-NSCD authorised device to the corporate network without permission (such as personal laptops), except when connecting to authorised guest systems where these exist.
- Store NSCD's data on any non-authorised equipment.
- Give or transfer NSCD's data or software to any other person or organisation outside of NSCD without the authority of a member of senior management and/or the IT department.

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

INTERNET, SOCIAL MEDIA AND EMAIL - CONDITIONS OF USE
The use of internet, social media and email is intended for work use and/or to aid in studies. Personal use is permitted where such use does not affect the individual's work/study performance (i.e. at lunchtime), is not detrimental to NSCD in any way, not in breach of any term and condition of employment and does not place the individual or NSCD in breach of statutory or other legal obligations.

All individuals are accountable for their actions on the internet, social media and email systems.

Individuals must not:
- Use the internet, social media or email for the purposes of harassment or abuse.
- Use the internet, social media or email to promote or encourage extremism or radicalisation.
- Use profanity, obscenities, or derogatory remarks in communications of any type.
- Access, download, send or receive any data (including images), which NSCD considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
- Use the internet or email to make personal gains or conduct a personal business.
- Use the internet or email to gamble.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Place any information on the Internet that relates to NSCD, alter any information about it, or express any opinion about NSCD, unless they are specifically authorised to do so.
- Send unprotected sensitive or confidential information externally.
- Forward confidential NSCD (internal) mail to personal (non-NSCD email accounts for example an external personal hotmail account).
- Make official commitments through the internet or email on behalf of NSCD unless authorised to do so.
- Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.
- Download any software from the internet without prior approval of the IT Department.
- Connect NSCD devices to the internet using non-standard connections.

CLEAR DESK AND CLEAR SCREEN POLICY
In order to reduce the risk of unauthorised access or loss of information, NSCD enforces a clear desk and screen policy as follows:

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

WORKING OFF-SITE
It is accepted that laptops and mobile devices will be taken off-site. The following controls must be applied:

- Equipment and media taken off-site must not be left unattended in public places and not left in sight in a car.
- Laptops must be carried as hand luggage when travelling.
- Information should be protected against loss or compromise when working remotely (for example at home or in public places).
- Remote access (staff only) is the preferred method for working offsite. When using remote access, all data remains onsite where it is safe.
- All NSCD laptops are configured, by default, for use with remote access.
- Particular care should be taken with the use of mobile devices such as laptops, mobile phones, smartphones and tablets. They must be protected at least by a password or a PIN and, where available, encryption.

MOBILE STORAGE DEVICES
Mobile devices such as memory sticks, CDs, DVDs and removable hard drives must be used only in situations when network connectivity is unavailable or when extra storage capacity is needed – for example video files.

Remote access should be used when working off site (where practical). No data should be taken offsite on mobile storage devices for security and data protection reasons without permission and should be disposed securely.

Only NSCD - authorised mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

CONFIDENTIALITY AND DATA
NSCD believes that protecting the privacy of our staff, students and parents/carers and regulating their safety through data management, control and evaluation is vital.

Members of staff have access to confidential information about students, other staff and parents/carers in order to undertake their daily duties, this may sometimes include highly sensitive information. This information must not be shared outside of NSCD or with external parties unless a student is at risk of harm or significant harm or there is an agreed multi-agency plan around a family and student, which means that sharing of information is in the best interests of the student.

NSCD takes responsibility for ensuring that any data collected is used correctly and only as is necessary, and the school will keep staff, students, parents/carers fully informed of how the data is collected, what is collected, and how it is used.

Attendance, assessment data, registration records, SEND data, and any relevant medical information are examples of the type of data that NSCD will capture. Through effective data management we can monitor a range of provisions and evaluate the wellbeing and academic progression of students to ensure that they receive an exceptional education and to respond to the changing needs of students.

In line with the General Data Protection Regulations (GDPR) 2016 and the NSCD's Data Protection Policy we will follow the principles of good practice when processing data. NSCD will ensure that data is fairly and lawfully processed and only for limited purposes. The school will ensure that all data processed is adequate, relevant, accurate and not excessive. Data will only be kept for the regulated period. It will be

processed in accordance with the data subject's rights and will always be secure and not transferred to other countries without adequate protection.

There may be circumstances where NSCD is required either by law or in the best interests of our students/staff to pass information onto external agencies or authorities; for example, Children's / Adult's Social Work Services. These authorities are up to date with GDPE and have their own policies relating to the protection of any data that they receive or collect.

ITC Manager is responsible for reviewing and managing the security of the computers and internet networks. NSCD takes the protection of data seriously and school's networks are protected, as far as is practicably possible, against viruses, hackers and other external security threats. The security of the information systems and users will be reviewed regularly by ITC Manager, and virus protection software will be updated regularly.

SOFTWARE
Users must use only software that is authorised by NSCD on NSCD's computers. Authorised software must be used in accordance with the software supplier's licensing agreements. All software on NSCD computers must be approved by the IT Manager.

INDIVIDUALS MUST NOT:

- Store personal files such as music, video, photographs or games on NSCD IT equipment.

VIRUSES
The IT department has implemented centralised, automated virus detection and virus software updates. All PCs have antivirus software installed to detect and remove any virus automatically.

INDIVIDUALS MUST NOT:

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

ACTIONS UPON TERMINATION OF CONTRACT
All NSCD equipment and data, for example laptops and mobile devices including telephones, smartphones, USB memory devices and CDs/DVDs, must be returned at termination of contract.

All NSCD data or intellectual property developed or gained during the period of employment remains the property of NSCD unless stated otherwise in the original contract.

MONITORING AND FILTERING
All data that is created and stored on NSCD computers is the property of NSCD and there is no official provision for individual data privacy, however wherever possible NSCD will avoid opening personal emails. IT system logging will take place where appropriate, and investigations will be commenced where reasonable suspicion exists of a breach of this or any other policy.

NSCD has the right (under certain conditions) to monitor activity on its systems, including internet, email and social media use, in order to ensure systems security and effective operation, and to protect against misuse.

Any monitoring will be carried out in accordance with audited, controlled internal processes, 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 use of the internet. This includes NSCD obligations under Prevent. Examples of content filtering include filtering by website categorisation, website blacklisting and website whitelisting.

This policy must be read in conjunction with:

- NSCD Safeguarding Policy

- NSCD Prevent Strategy
- NSCD E Safety and Online Policy
- School Policy on Handling and Storage of Security Sensitive Materials
- Staff & Student Codes of Conduct

Applicable laws, primary Acts of Parliament and policies which relate to and/or govern the provision and use of IT facilities include:

- 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
- Copyright and Trademarks (Offences and Enforcement) Act 2002
- The Telecommunications Act (1984)
- The Electronic Communications Act (2000)
- Obscene Publication Act 1959 & 1964
- Protection of Children Act 1978
- The Defamation Act (1996 and 2013)
- Police and Criminal Evidence Act 1984
- Police and Justice Act 2006
- Prevention of Terrorism Act 2005
- Terrorism Act 2006
- Counter Terrorism and Security Act 2015
- Human Rights Act 1998
- Equality Act 2010
- Privacy and Electronic Communications Regulations 2003

** This list is not exhaustive and will be subject to change **

It is your responsibility to report suspected breaches of security policy without delay to your line management or the IT department.

All breaches of information security policies will be investigated. Where investigations reveal misconduct, disciplinary action may follow in line with NSCD disciplinary procedures.

USER AGREEMENT FORM – NSCD COPY

This form relates to the Acceptable Use Policy (AUP), to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Policy.

If you do not sign and return this agreement, access cannot be granted to NSCD IT systems.

If you have any questions regarding the Acceptable Use Policy, please contact your line manager or a member of the IT department.

I have read and understand the above and agree to follow these guidelines when using NSCD IT systems when either on-site or off-site.

Name (Printed): ……

Date: …….

Job Title: ……

Signature: …….

Once signed, please pass it on to your line manager, the IT department or the HR department to be added to your employment record.

USER AGREEMENT FORM – USER COPY

This form relates to the Acceptable Use Policy (AUP), to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Policy.

If you do not sign this agreement, access cannot be granted to NSCD IT systems.

If you have any questions regarding the Acceptable Use Policy, please contact your line manager or a member of the IT department.

I have read and understand the above and agree to follow these guidelines when using NSCD IT systems when either on-site or off-site.

Name (Printed): ……

Date: …….

Job Title: ……

Signature: …….

Please keep this page along with a copy of the acceptable use policy for your records.