Acceptable Use Policy for IT Systems

Introduction

This Acceptable Use Policy (AUP) for IT Systems is designed to protect the National Centre for Circus Arts, 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 National Centre for Circus Arts 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, head of academic administration and student support or a year Manager.

Definitions

NCCA is an abbreviation of the establishment's name, the National Centre for Circus Arts.

"Users" are everyone who has access to any of NCCA'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 similar 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 NCCA'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.

NCCA has a statutory duty, under the Counter Terrorism and Security Act 2015, which is termed PREVENT. The purpose of this duty is to aid the process of preventing people being drawn into terrorism. This Prevent duty informs its policy on the acceptable use of IT systems.

Staff members at NCCA who monitor and enforce compliance with this policy are responsible for ensuring that they remain compliant with relevant local legislation at all times. More information can be found in the Prevent E-Safety Measures document on the NC-Cloud for staff or in MS TEAMS for students.

Links to local laws and legislation relating to this document are provided at the end of this document.

USE OF IT SYSTEMS

Computer Access Control – Individual's Responsibility
Access to NCCA'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 NCCA'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-NCCA authorised device to the corporate network or IT systems (such as personal laptops), except when connecting to authorised guest systems where these exist.
- Store NCCA data on any non-authorised equipment.
- Give or transfer NCCA data or software to any other person or organisation outside of NCCA without the authority of a member of senior management.

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 NCCA in any way, not in breach of any term and condition of employment and does not place the individual or NCCA 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 NCCA 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 NCCA, alter any information about it, or express any opinion about NCCA, unless they are specifically authorised to do so.
- Send unprotected sensitive or confidential information externally.
- Forward NCCA (internal) mail to personal (non-NCCA email accounts (for example an external personal hotmail account).
- Make official commitments through the internet or email on behalf of NCCA 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.
- Connect NCCA 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, NCCA 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 NCCA 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. Remote access should

be used when working from home (staff only). No data should be taken offsite on mobile storage devices for security and data protection reasons.
- Only NCCA authorised mobile storage devices with encryption enabled must be used, when transferring sensitive or confidential data.

Software
Users must use only software that is authorised by NCCA on NCCA's computers. Authorised software must be used in accordance with the software supplier's licensing agreements. All software on NCCA computers must be approved and installed by the IT department.

Individuals must not:
- Store personal files such as music, video, photographs or games on NCCA IT equipment.

Viruses
The IT department (SpirIT UK) 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 by the use of approved anti-virus software and procedures.

Actions upon Termination of Contract
- All NCCA 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 NCCA data or intellectual property developed or gained during the period of employment remains the property of NCCA and must not be retained beyond termination or reused for any other purpose.

Monitoring and Filtering
- All data that is created and stored on NCCA computers is the property of NCCA and there is no official provision for individual data privacy, however wherever possible NCCA 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.
- NCCA 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.

NCCA employs filtering of web content. Examples of content filtered include:

Hacking
Weapons
Hate & racism
Violence
Illegal

This policy must be read in conjunction with:

Computer Misuse Act 1990
Data Protection Act 1998
Regulation of Investigatory Powers Act 2000
Telecommunications (Lawful Business Practice Interception of Communications) Regulations 2000
Terrorism Act 2006
Counter-Terrorism and Security Act 2015
NCCA safeguarding policy
NCCA Prevent Strategy and Policy.

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 NCCA disciplinary procedures.

Effective Date: 17/10/2017
Revision Date: 22/09/2022