January 2022

NATD

National Association of Teachers of Dancing

IT Security Policy

1. Introduction

1.1 This policy defines a framework by which NATD computer systems, assets, infrastructure and computing environment will be protected from threats whether internal, external, deliberate or accidental.

2. Key Principles

2.1 All central computer systems, environments and information contained within them will be protected against unlawful access by using secure user accounts with strong passwords.

2.2 Information kept within these systems will be managed securely, to comply with relevant data protection laws and to satisfy NATD expectations that such assets will be managed in a professional, safe and dependable manner. Security review is a permanent item on the GP&F agenda.

2.3 NATD employees are required to familiarise themselves with this policy, to adhere to it and comply with its requirements. Cyber Training and group discussions have been provided to staff using the NCSC Online Training Program.

2.4 The Administration Manager has a responsibility for ensuring the implementation of, adherence to and compliance with this policy throughout their areas of functional responsibility. Security training is part of any new staff induction

2.5 The integrity of the computer system, the confidentiality of any information contained within or accessible on or via these systems is the responsibility of NATD.

2.6 All regulatory and legislative requirements regarding computer security and IT based information confidentiality and integrity will be addressed by NATD. Awareness of good practice is raised by external organisations such as CDMT/BDC/S&RA.

2.7 All breaches of security will be reported to and initially investigated by the Administration Manager and reported immediately to the CEO.

2.8 All employees have a responsibility to report promptly to the Administration Manager any incidents which may have an IT security implication for NATD. This process has been proven to work well.

3. The Computing Environment

3.1 The computing environment is defined as Head Office computing resources and network infrastructure managed and overseen by NATD and all computing devices that can physically connect to it. All are covered by this policy, including computing hardware and software, any NATD related data residing on these machines or accessible from these machines within the network environment, including media such as external storage devices, USB drives, memory cards, CDs, DVDs, and backup devices.

3.2 All temporary and permanent connections, including laptop docking points, Wi-Fi connections, and remote connections using VPNs etc. are similarly subject to the conditions of this policy.

3.3 Head Office reserves the right to monitor, log, collect and analyse the content of all transmissions on networks maintained by NATD at any time deemed necessary for performance, fault diagnostic and IT compliance purposes.

4 Physical Security

4.1 NATD provides a secure server room facility with protected power arrangements and a climate-controlled environment.

4.2 Any computer equipment in general office environments must be secured behind locked doors, protected by user log-out and password protected screensavers whenever it is left unattended, and outside of general office hours.

4.3 Any portable equipment such as laptops and tablets should use a log-on or power-on password wherever possible. Any unattended portable equipment should be physically secure, for example locked in an office or a desk drawer. When being transported in a vehicle they should be hidden from view. Staff should avoid storing sensitive information on portable equipment whenever possible (see data security section, at 5. below).

4.4 Staff who store confidential information on NATD owned portable equipment must ensure that such data is thoroughly and securely cleansed from that equipment when they leave NATD employment. This is covered and confirmed as part of the Exit Interview.

5. Data Security

5.1 NATD attaches great importance to the secure management of the data it holds and generates and will hold staff accountable for any inappropriate mismanagement or loss of it.

5.2 NATD holds a variety of sensitive data including personal information about students and employees. If staff members have been given access to this information, they must be aware of their responsibilities under current data protection law.

5.3 NATD provides secure and practical remote access to information and data held within its various systems environments and IT infrastructure. In most cases, gaining access to such data from an offsite point of electronic access will prove sufficient – and safe - for most needs and is the recommended general mode of remote use of such data and information.

5.4 Any copying – or original creation – of sensitive data and information onto any form of portable media transport device or mechanism (Memory Stick, CD, DVD, External Hard Drive, PDA, portable music player, laptop, etc.) or its transportation beyond the secure environment it was intended to be used within (systems environment, PC environment, office etc.) carries additional responsibilities for the individual undertaking such activity.

5.5 Employee/Student/Teacher/Patron (personal) data should never leave Head Office. In this context “leave” implies its physical transport to an external, and insecure location. Remote access to such data through an individuals approved access levels and permissions is distinct and not intended to be included in the term “leave”.

6. Loss or Theft of Confidential Information

6.1 All incidences of loss or theft of confidential information should be reported immediately to the Office Manager so that they may be investigated. A data or IT security incident relating to breaches of security and/or confidentiality could range from computer users sharing passwords to the loss or theft of confidential information

6.2 A security incident is any event that has resulted or could result in:

6.2.1 The disclosure of confidential information to any unauthorised person.

6.2.2 The integrity of the system or data being put at risk.

6.2.3 The availability of the system or information being put at risk.

6.2.4 Adverse impact, e.g.

6.2.4.1 Negative impact on the reputation of NATD.

6.2.4.2 Threat to personal safety or privacy.

6.2.4.3 Legal obligation or penalty.

6.2.4.4 Financial loss or disruption of activities.

6.3 All incidents must be reported to the Administration Manager. Serious incidents should be reported immediately to the CEO. A written report should be submitted containing the following information:

6.3.1 Details of the incident.

6.3.2 Date of discovery of the incident.

6.3.3 Place of the incident.

6.3.4 Who discovered the incident.

6.3.5 Category/classification of the incident.

6.3.6 Action already taken if risk to the organisation.

6.3.7 Any action taken by the person discovering the incident at the time of discovery, e.g., report to police.

6.4 In the case of a serious potential breach, the CEO will instigate an investigation into the incident and will decide whether it needs to be reported to any regulatory bodies, e g Ofqual or other third parties.

6.5 The following is a list of examples of breaches of security and breaches of confidentiality. It is neither exclusive nor exhaustive and should be used as a guide only. If there is any doubt as to what constitutes an incident, it is better to inform the Administration Manager immediately who will then decide whether a report should be made.

6.6 Examples of breach of security:-

6.6.1 Loss of computer equipment due to carelessness.

6.6.2 Loss of portable media devices, e.g. – memory sticks etc.

6.6.3 Accessing any part of a database using someone else's password.

6.6.4 Finding doors and/or windows broken and/or forced entry gained to a secure room/building in which computer equipment exists.

6.7 Examples of a breach of confidentiality:-

6.7.1 Finding any records about an employee, patron, teacher or student, in any external location

6.7.2 Passing information to unauthorised people either verbally, written or electronically.

7. Specific Systems

7.1 Computer and network systems access is only via individual user accounts.

7.2 Email

7.2.1 Email is not a completely secure medium. Staff should be conscious of this and consider how emails might be used by others. Remember that emails can easily be taken out of context that once an email is sent there is no control over what the recipients might do with it, and that it is very easy to forward large amounts of information.

7.2.2 Similarly recipients should not necessarily trust what is received in an email - in particular, never respond to an email request to give a username or password.

Always think before you click a link. Check the sender's e mail address.

7.3 File Storage

7.3.1 For the vast majority of applications the security of files stored centrally is appropriate. This means they will be backed up as part of a nightly backup routine. The backup routine stores data locally on-site to a Network Attached Storage Device, and copies are also automatically stored nightly off-site using a secure cloud-based solution.

7.4 The Web

7.4.1 Users should consider the security implications of any information they put on the NATD web-site and social media sites. NATD reserves the right to remove any material which it deems inappropriate, illegal or offensive.

7.4.2 Users shall not in any way use web space to publish material which undermines IT security at NATD. In particular this covers making information available about how IT security is implemented at a practical level, or any known weaknesses.

7.5 Remote Access to Systems

7.5.1 Remote access is defined as accessing systems from a physically separate network. This may include:

7.5.1.1 Connections direct across the Internet

7.5.1.2 VPN Connections

7.5.2. Remote access is allowed via secure methods only.

Head Office shall provide the only VPN that may be used.

7.5.3 All connections via these services will be logged. No other remote access service shall be installed or set up, including single connections to servers or workstations.

7.6 Anti-Virus Security

7.6.1 NATD will provide means by which all employees can download and install current versions of site-licensed virus protection software.

7.6.2 Users must ensure that they are running with adequate and up-to-date anti-virus software at all times. If any user suspects viral infection on their machine, a complete virus scan should be performed. If NATD detect a machine behaving abnormally due to a possible viral infection it will be disconnected from the network until deemed safe. Reconnection will usually only be after liaison with local IT support.