NATD

National Association of Teachers of Dancing

IT SECURITY POLICY

VERSION	APPROVAL DATE	CLASSIFICATION
2.0	June 2026	CONFIDENTIAL

NATD 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, strong passwords and multifactor authentication where possible.

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.

2.3 All NATD employees are required to familiarise themselves with this policy, to adhere to it and comply with its requirements. Security awareness and familiarization with this document are part of any new staff induction.

2.4 The IT Consultant and the Administration Manager based at NATD HO have responsibility for ensuring the implementation of, adherence to and compliance with this policy throughout their areas of functional responsibility.

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 breaches of security will be reported to and initially investigated by the IT Consultant and reported immediately to the CEO

2.7 All employees have a responsibility to report promptly to the IT Consultantant incidents which may have an IT security implication for NATD.

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 An IT Asset register of all equipment will be kept by the IT IT Consultant both electronically in a secure database, and in paper form in the IT file, kept securely in the IT room at Head Office, Turnfields Court, Thatcham, Berkshire, RG19 4PT

3.3 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.

3.4 The NATD reserve the right to monitor, log, collect and analyse the content of any transmissions on networks maintained by themselves if necessary for security, performance, fault diagnostic or IT compliance purposes.

4 Physical Security

4.1 NATD provides a secure server room facility for file servers and network storage devices. This room provides 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 must use a log-on and/or power-on password 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 removed from that equipment when they leave NATD employment.

5. Data Security

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

5.2 Only the IT Consultant is permitted to install software and make changes to IT devices. Users requiring access to software or apps not installed on their devices must first discuss their case with the IT Consultant, and NOT attempt to download or install any new software themselves.

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

5.4 Staff using PCs and Laptops must all have unique login names together with strong passwords. These passwords should be changed every 6 months, or immediately if the user suspects their password is known to others. Passwords should be at least 8 characters in length and contain both uppercase and lowercase letters, numbers and symbols.

5.5 It is the user's responsibility to ensure the IT Consultant is kept informed of any password changes as soon as they occur. This should be done verbally and NOT in an email. These passwords will be stored (in an encrypted and unreadable format) inside the IT Asset Database, available only to the IT Consultant should the need arise to use them.

5.6 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, 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.

5.7 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 incidents of loss or theft of confidential information should be reported immediately to the IT Consultant 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 – for example:-

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 IT Consultant. 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 including date & time of discovery.
6.3.2 Place of the incident.
6.3.3 Who discovered the incident.
6.3.4 Category/classification of the incident.
6.3.5 Action already taken if risk to the organisation.
6.3.6 Any action taken by the person discovering the incident at the time.

6.4 In the case of a serious potential breach, the IT Consultant & CEO will instigate an investigation into the incident and will decide whether it needs to be reported to any regulatory bodies.

6.5 The following is a list of some typical examples of breaches of security and breaches of confidentiality. If there is any doubt as to what constitutes an incident, it is better to inform the IT Consultant 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 should only be made 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. Emails can easily be taken out of context and once sent, there is no control over what the recipient might do with the contents. It is also 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 requesting personal information, especially usernames and/or passwords or anything financial. Always think before you click a link. Check the sender's e mail address.

(For more information about the NATD's use of hosted Exchange Server and mail software configuration, see the separate *Email System Technical Notes* document.)

7.3 File Storage:-

7.3.1 For the vast majority of applications, the security of files stored centrally on the NATD's file server and storage devices is appropriate. The files 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.

7.3.2 Users are discouraged from storing data files on local drives and physical external storage devices (USB drives etc) because it poses both a security risk, and the data itself will not be backed up in the same way it would if the data was stored on the central file server.

7.3.3 When necessary, users can save data to their own personal secure OneDrive folder setup by the IT Consultant.

(For additional information concerning specific backup routines and schedules see the separate *IT Back Up Technical Notes* document.)

7.4 The Web:-

7.4.1 Users should consider the security implications of any information they put on the NATD website 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 any way.

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 only permitted using secure methods provided to the users by the IT Consultant.

(For additional information about remote access methods see the separate *Remote Access Technical Notes* document.)

7.6 Anti-Virus & Security Software:-

7.6.1 NATD will provide the means and software by which all their IT equipment is protected. Regular checks will be made on all equipment to ensure that security software is current and working correctly.

7.6.2 If any user suspects cyber infection on their machine or any other security threat, they must contact the IT Consultant immediately and disconnect the device from the network. Reconnection will only happen once the device is considered safe, in conjunction with support from the IT Consultant.

(For more information about the specific AntiVirus and Security software used by NATD, see the separate *IT Security Software Technical Notes* document.)