National Institute *of* Dramatic Art NIDA

INFORMATION AND COMMUNICATION TECHNOLOGY POLICY

POLICY AND PROCEDURE ON ACCEPTABLE USE OF NIDA INFORMATION AND COMMUNICATION TECHNOLOGY AND EMAIL RESOURCES

1. Preamble	Information and communications technology (ICT) has become of critical importance to NIDA in the support of teaching and learning, research, core business activities and communications. In recognition of this, NIDA provides computing, email, internet and communication facilities to its staff and computing and email facilities to its students for the purposes of research, teaching and learning, and to support the administration of NIDA. This policy and procedure informs users of NIDA ICT resources of their rights and responsibilities, and of NIDA's requirement that its ICT resources are used in a legal, ethical, responsible and appropriate manner. This policy and procedure also applies to the use of information that may be accessed via NIDA's ICT resources, and supports the NIDA Code of Conduct, which sets out the general rules of conduct for staff of NIDA. While NIDA upholds the principles of academic freedom, it will not condone deliberate breach of either NIDA policies or external legislative requirements, and will cooperate fully with the authorities in any investigations resulting from a breach. Consequences of a breach may include the removal of access rights to NIDA's ICT resources, disciplinary proceedings, and in the case of serious and deliberate breach, may result in civil or criminal proceedings. Situations not listed here will inevitably arise, and they should be interpreted according to the spirit of this policy. **1.1 Principles** The following principles express the general intent of this policy and procedure: 1.1.1 NIDA will provide access to information and communications technology resources, including email access, to eligible persons according to need and available resources. 1.1.2 NIDA requires legal, ethical, responsible and appropriate use of its ICT resources.

	1.1.3 NIDA will take every precaution to protect the security and privacy of its users' ICT accounts, but users should be aware that normal operation and maintenance of systems includes backup, logging of activity and monitoring of general usage patterns. In addition, NIDA may be legally required to provide copies of electronic records / communications under subpoena or other legal orders. 1.1.4 NIDA values and respects the principles of academic freedom and freedom of expression, requiring that these be exercised responsibly. **1.2 Disclaimer** While NIDA will make every effort to ensure the availability and integrity of its ICT resources, it cannot guarantee that these will always be available, and / or free of any defects, including malicious software (e.g. computer viruses). Users should take this into account when accessing the resources. NIDA uses Google for student email accounts. Google Apps including email used by students is not backed up by NIDA and are subject to Google's terms and conditions of use that may change regularly. Google may target students with advertising, and the location of email content is unknown. Each student user is responsible for checking Google's terms and conditions including control of user content and indemnity.
2. Scope	This is a NIDA-wide procedure which applies to all users of NIDA ICT resources – including (but not limited to) staff, students, contractors, third parties, alumni, associates and honoraries and visitors to NIDA. The policy also applies to anyone connecting personally-owned equipment (e.g. laptops, USB memory sticks, external hard drives, personal digital assistants, CDs/DVDs, MP3 player, IPods and mobile phones) to the NIDA network. It is important to acknowledge here the dual role of IT professional staff as both IT system administrators and as staff who are also 'standard ICT users'. This policy will apply to those staff while in their role as 'standard ICT users'. However, in the course of their professional duties, IT staff may be required to undertake actions which are beyond those permitted in this policy. It is expected that they will do so in the spirit of both NIDA's Code of Conduct and appropriate professional Codes of Ethics, such as that of the System Administrators Guild of Australia. See www.sage-au.org.au
3. Definitions	For purposes of this policy, unless otherwise stated, the following

	definitions shall apply: **An Account** Any computing or electronic communication resource allocated to a user by NIDA and protected from general usage by a security system (e.g. password). **ICT (Information and Communications Technology)** ICT includes technologies such as desktop and laptop computers, PDA's, software, peripherals, telephone equipment (including mobile phones) and connections to the internet that are intended to fulfil information processing and communications functions. It also includes having access to a NIDA email address, when appropriate. **NIDA ICT Resources** (i) All networks, hardware, software and communication services and devices which are owned, leased or used under licence by NIDA including NIDA's teaching and administrative systems; and (ii) Computing facilities and information resources maintained by other bodies, but available for use through an agreement or agreements with NIDA. **NIDA Network** NIDA's IT network and other networks provided by NIDA. Non-NIDA facilities and equipment (e.g. personally-owned computers) which are connected to the NIDA network will, for the purposes of this document, be considered to be part of the NIDA network. **User, Authorised User** 'User' and 'Authorised User' means and includes all staff, students, alumni and other users who are authorised by NIDA to access its systems and / or network.
4. Policy Statements and Procedures	**4.1. Provision of ICT Resources** NIDA recognises the importance of computing and communication technologies and will provide access to ICT resources for its staff, students and other authorised users, for the purposes of research, teaching, learning and administration. NIDA will provide eligible users with access to the ICT resources required to perform their work, research or studies, according to need and available resources. Email accounts will be available centrally to all students enrolled in the full-time courses and all staff. Access to the service will be terminated when the user ceases to be an employee or enrolled student of NIDA. NIDA reserves the right to terminate the access of any user whom it believes is not operating in accordance with

NIDA policies and procedures.

4.2. Legal, Ethical, Responsible and Appropriate Use of ICT Resources

NIDA requires all users of its ICT resources to do so in a legal, ethical, responsible and appropriate manner. Users of NIDA ICT resources must be aware that use of these facilities is subject to the full range of State and Federal laws that apply to communications and to the use of computers, as well as any other relevant laws and NIDA policies and procedures.

This includes (but is not limited to) copyright, intellectual property, breach of confidence, breach of privacy, defamation, contempt of court, harassment, vilification and anti-discrimination legislation, the creation of contractual obligations, civil and criminal laws. In addition, NIDA's ICT resources must not be used for unauthorised commercial activities or unauthorised personal gain. Use of its ICT resources must not cause loss of service, or risk loss of reputation to NIDA. Actions performed using NIDA's computer and network resources, regardless of any disclaimers that might be made, ultimately reflect on the NIDA community as a whole. In particular, NIDA's ICT resources must not be used to copy, download, store or transmit material which infringes copyright, such as music files, movies, videos etc. Actions performed using NIDA ICT resources must comply with the terms of any licence signed by NIDA including, but not limited to, for use of online databases, software programs, online publisher packages etc.

4.2.1. Respect for Intellectual Property and Copyright

Although the Internet allows easy access to information, images, musical recordings, films, videos, software and other intellectual property, it does not mean these things are therefore freely available to copy or download. Much material is accessible on the internet without the copyright owner's permission. NIDA's ICT resources must not be used to copy, download, store or transmit material which infringes copyright. Users of NIDA ICT resources are responsible for complying with copyright law.

Users will respect the copyright and intellectual property rights of others by action such as:

- using only appropriately licensed and authorised computer software programs
- Complying with the terms of any license signed by NIDA for online databases, software programs, online publisher packages, etc.
- Ensuring copyright material is only copied or used with the permission of the copyright owner, under the terms of a copyright licensing agreement, or as permitted by law.

Examples of inappropriate use include (but are not limited to):

- Making / using illegal copies of a licensed computer program
- Downloading, copying, storing or transmitting material such as music, video or movie files, without the express permission of the copyright holder or as permitted by law
- Downloading material unrelated to teaching, learning or research which incurs significant additional cost to NIDA.

4.2.2. Use ICT Resources Efficiently and Professionally

Computing resources are finite and must be shared by many. Therefore, users should ensure they are efficient and professional in their use of the network facilities, services and applications they are required to use in their positions.

Examples of efficient and professional use include:

- Communication of work-related information (e.g. email) is expressed with the same professional care and courtesy as is given to a signed paper memo
- Users receive appropriate training in the applications they are required to use in their daily work
- Users ensure that personal incidental use of ICT resources is kept to a reasonable minimum (see section 4.2.5 for examples of acceptable personal incidental use).

Examples of inappropriate use include (but are not limited to):

- Downloading large files beyond the 5GB download limit per month without permission ("hogging" bandwidth)
- Excessive printing using a shared facility
- Excessive personal use of ICT resources
- Eating, drinking or making undue excessive noise in a shared computing facility (e.g. a computer laboratory) where this is not permitted.

Performance and cost of the electronic mail systems for all users can be adversely affected by inconsiderate use by particular individuals. Therefore NIDA reserves the right to set limits on the size of individual electronic mail items sent, the total volume of electronic mail sent and the amount of electronic mail retained on the central electronic mail servers.

NIDA pays for electronic mail incoming to NIDA. While clearly in most cases users are not responsible for the electronic mail sent to them, they may encourage such mail. Therefore users should not solicit large volumes of incoming mail with no, or marginal relevance to their role within NIDA. NIDA reserves the right to request that users unsubscribe from external mailing lists where unacceptable costs are incurred.

NIDA also reserves the right to block email containing computer

	viruses or worms, material not relevant to NIDA, unsolicited email or email which causes performance or security issues to NIDA email servers. 4.2.3. Use of ICT Resources and Email in a Legal and Appropriate Manner Examples of unlawful / inappropriate use of NIDA ICT resources include (but are not limited to): • Creating / sending email under another's name (forgery) • Creating / sending / forwarding electronic chain letters, • Unsolicited broadcast emails (Spam), obscene, abusive, fraudulent, threatening or repetitive messages • Using ICT resources, including email, to harass, threaten, defame, vilify or discriminate against any individual or group • Using a NIDA email address for commercial purposes or in a manner inconsistent with the relationship that the individual user has to NIDA • Intentional or irresponsible damage of ICT resources • Stealing equipment • Connecting a device to the NIDA network which is configured to breach this policy • Accessing gambling or gaming sites or material that is obscene, pornographic, pedophilic, and discriminatory or vilificatory, that promotes illegal acts, or that advocates violence • Using ICT resources to obtain, store, display copy or transmit potentially unlawful or obscene material • Using NIDA email to send private or confidential information • Accessing, damaging or interfering with NIDA's IT infrastructure and equipment. • Under no circumstances may NIDA ICT resources be used for, or in relation to, corrupt conduct, unauthorised personal financial or commercial gain, or for the unauthorised financial or commercial gain of a third party. It is acknowledged that access to potentially unlawful or inappropriate material may be required for legitimate research and teaching purposes. However, access to this material remains inappropriate UNLESS it has been authorised in writing by the Director / CEO or Director, Student & Staff Services as legitimately required for teaching and / or research purposes as a requisite component of an approved course of study or research program, AND access to the material is restricted to legitimate users. 4.2.4. Access by Minors The Broadcasting Services Act (1992) requires that Internet service providers obtain permission from parents or guardians before providing a user account to a person under 18 years of

	age (including university students). Departments, such as NIDA Open, which run programs for minors which involve internet access, can cover this likelihood by ensuring that the school or parent permission slip, as the case may be, includes reference to parent/carer permission to access to the Internet. 4.2.5. Limited Incidental Personal Use While NIDA ICT resources are provided for the purposes of teaching, learning, research and NIDA administration, limited incidental personal use is allowed, so long as such use: • Is lawful and compliant with NIDA policies and external legislation • Does not negatively impact upon the user's work performance • Does not hinder the work of others or interfere with the normal operations of the network • Does not damage the reputation or operations of NIDA, and does not impose unreasonable or excessive additional costs on NIDA. Examples of acceptable limited incidental personal use include: • An online personal banking transaction • An online airline schedule • Enquiry or booking and • Checking "home" personal email accounts. 4.2.6. Email directories, mailing lists and broadcasts • To limit the quantities of unsolicited email, members of NIDA must not provide external organisations with copies of directories or lists of the email addresses of NIDA students or staff • Unsolicited email may only be sent to multiple users where the mailing is related to their NIDA function and the sender has an appropriate work relationship. Special interest groups must issue invitations to join before including any group or individual in a mailing list, and members must have the right to unsubscribe at will • Sending of unsolicited broadcast emails to all NIDA students or staff requires the approval of the Director / CEO or Director, Student & Staff Services (for all NIDA students) and the Head of Course (for all members of a course). **4.3. Security and Privacy** While NIDA will take every precaution to protect the security and privacy of its users' ICT accounts, users should be aware that NIDA policies and procedures require retention and inspection of

	some electronic files and communications held on NIDA's systems. ICT systems email and internet use may be monitored. Such monitoring will be in accordance with the Privacy Act and the Workplace Surveillance Act. Network and systems administrators treat the content of electronic communications and data as confidential. However, users must be aware that recordkeeping and normal operation and maintenance of the systems generally requires backup and caching of communications and data, the logging of activity, and monitoring of general usage patterns. Since privacy obligations are often defined by situation and circumstances, NIDA cannot guarantee absolute privacy to users of its ICT resources. NIDA may be required to inspect or provide copies of electronic communications under law, or when investigating possible misuse of ICT resources. Users should be aware that electronic records may be subject to NIDA's obligation to respond to subpoenas or other legal orders. For example, email is considered a document under the law and can be legally requested, as can any other document. NIDA has a responsibility to ensure the service it provides is used appropriately, and in order to do so may exercise its legal right to read any electronic mail sent via its systems. NIDA may also impose security procedures deemed necessary and appropriate to maintain the security and privacy of its ICT resources, including requiring users to change passwords on a regular basis. Users who have legitimate access to personal and confidential information must respect the privacy of others and maintain the confidentiality of the information to which they have access. Users will protect computer systems including laptops and other portable devices, information and accounts by: • Choosing "strong" passwords and / or changing passwords periodically (a "strong" password is one that is hard for others to guess; it should contain a mixture of letters and numbers and should not be as simple as a birth date or a pet's name) • Keeping their log-in details confidential; users are responsible for all activities occurring using their accounts • Using their access only as authorised • Respecting the privacy and confidentiality of information to which they may have access • Using and keeping up-to-date recommended anti-virus programs and operating system / security patches • Downloading, installing or using only authorised and licensed software programs • Not copying private or sensitive information to personal devices when remotely accessing NIDA's ICT systems

	• Promptly reporting any breach or gap in system or network security to NIDA's IT Administrator • Performing virus check on email attachments and disks before opening. Examples of unacceptable use include (but are not limited to): • Allowing others to gain unauthorised access using your log-in or password • Passing on private or confidential information to persons not authorised to access that information • Gaining unauthorised access to systems by any means, including port scans, "hacking", and use of "password sniffer" software • Using NIDA ICT resources to attack or compromise any other system, whether on or off NIDA premises • Downloading, installing or using unauthorised / unlicensed software programs • Knowingly propagating or installing computer viruses or malicious code • Accessing or intercepting others' electronic communications without permission. When an employee leaves NIDA, supervisors will ensure that all access to NIDA administrative systems, networks, email accounts etc. is removed or amended as appropriate upon the employee's departure from NIDA. If there is to be a continuing relationship after exit (e.g. honorary appointment, alumnus) then appropriate access to ICT resources can be allocated as per need. It may be necessary for a supervisor to access work files or email accounts after an employee's departure from NIDA in order to preserve continuity of work. In these circumstances, a departing employee will normally be given the opportunity to remove any personal files or email from NIDA computers prior to their departure. Staff and students should be aware that electronic mail is not a secure form of communication, and that privacy and confidentially are not guaranteed. NIDA cannot guarantee the confidentiality of undiscovered alteration of electronic mail messages, sent internally or via the internet, unless steps are taken to guard against disclosure. It is the responsibility of the senders, recipients and managers of electronic mail systems to exercise due diligence to ensure the protection of confidential communications. While most users operate electronic mail in an ethical or legal manner, NIDA advises that forgery of electronic mail can and does occur in the current environment. Whether crude or sophisticated, it is recommended that, should electronic mail suggest an unusual course of action, recipients should seek to

verify the authenticity

of the message via some other form of communication; this may take place via personal contact, paper mail, fax or telephone or an authentication means.

4.4. Security of ICT Resources

NIDA will take all reasonable steps to protect its ICT resources, including infrastructure and data, from unauthorised or unacceptable use to ensure that accurate and complete information is accessible only to authorised users.

Users of ICT resources must not:

i. Modify the standard configuration of any ICT facility.
ii. Install or use unlicensed or malicious software or circumvent ICT security measures
iii. Connect unapproved networking devices to ICT facilities
iv. Leave sensitive resources, information or data unprotected.
v. Retain the same ICT password for extended periods
vi. Release ICT passwords to any other person.
vii. Dispose of ICT resources or data without the approval of the Manager, Information Technology.
viii. Use their access to ICT resources to gain any personal, academic or other advantage.
ix. Access, damage or interfere with NIDA's IT infrastructure and equipment.

4.5. Personal and Portable Devices (PSDs)

Personal and portable devices (PSDs) includes home-based desktop PCs, laptops, USB memory sticks, external hard drives, personal digital assistants, CDs/DVDs, MP3 player, IPods and mobile phones. The use of PSDs raises privacy and statutory compliance risks relating to personal information storage and security. Such devices may be lost, stolen, or misused, and information on them will be compromised.

- Personal or private NIDA-related information must not be stored on PSDs.
- Use 'strong' passwords to prevent unauthorised use of PSDs. Do not share PSDs.
- Never leave PSDs with NIDA-related information unattended or not physically secured.
- Immediately report any lost or stolen PSDs that contain NIDA related information.
- NIDA-related information must be fully erased from PSDs when the information is no longer required.
- Each staff member is personally responsible for information security of their PSDs.

	4.6. Academic Freedom and Freedom of Expression NIDA upholds the principles of academic freedom. It values the diversity of cultures, ideologies and perspectives within its community and is respectful of freedom of expression. NIDA does not condone censorship, nor does it endorse the inspection of electronic files other than on an exceptional basis (e.g. when required by law or when investigating a reported or suspected violation). The right to academic enquiry and freedom of expression is tempered by the rights of others, including privacy, freedom from intimidation, discrimination or harassment, protection of intellectual property and copyright and ownership of data and security of information. NIDA requires all users of its ICT resources to do so in a legal, ethical, appropriate and responsible manner, in accordance with this and other NIDA policies and procedures and relevant State and Federal legislation.
5. Legal and Policy Framework	Users of NIDA ICT resources must be aware that use of these facilities is subject to the full range of State and Federal laws that apply to communications and to the use of computers, as well as any other relevant laws and NIDA policies. This includes (but is not limited to) copyright, breach of confidence, defamation, privacy, contempt of court, harassment, vilification and anti-discrimination legislation, the creation of contractual obligations, and civil and criminal laws. NIDA does not permit its ICT resources to be used for unauthorised commercial activities, unauthorised private gain or that of others. Staff are referred to NIDA's Code of Conduct and students to NIDA's Student Code of Conduct. Users must not use 'cloud' internet-based applications to copy, transmit or store private or confidential information. Users should be aware that some third party applications licensed to NIDA may have their own Terms and Conditions which may apply over and above this policy and procedure.
6. Implementation	**6.1. Responsibilities** The Director, Operations has the responsibility for coordinating the implementation of this policy and its associated documents. **6.2. Compliance and Breaches** 6.2.1. Notifying Violations Staff and students who become aware of possible violations of this policy and procedure should report them immediately to an appropriate person, such as their supervisor, the NIDA IT

	Manager, the Director, Operations, the Director, Human Resources or Head of Department. Alleged serious or repeated breaches must be reported to the Director, Operations. In cases where personal safety may be at risk, unauthorised entry to a computing facility has occurred or, where it is believed necessary to seize material held on a NIDA computer, the Director, Operations should be contacted for advice and assistance. 6.2.2. External Requests for Information If a request is received from an external organisation for information held on NIDA computers (e.g. copies of emails or other correspondence) it must be passed immediately to NIDA's Director Student and Staff Services for investigation and action. 6.2.3. Penalties Associated with Violations Penalties will depend upon the type and severity of breach. Penalties may range from loss or restriction of access, to formal NIDA disciplinary action under Student Misconduct Procedures or for staff for breach of the NIDA Code of Conduct. Cases of serious, deliberate, and / or criminal breach will be referred to external authorities and may result in civil or criminal proceedings. NIDA reserves the right to limit access to its networks provided through NIDA-owned or other computers and to remove or limit access to material and resources stored on NIDA-owned computers.
7. Review	It is anticipated that this policy will be reviewed every two years.
8. Acknowledgement	NIDA acknowledges the UNSW policy and procedure documents on acceptable use of ICT resources and email as significant source documents for the development of this policy.
Related policies, procedures and documents	• NIDA Staff Code of Conduct • NIDA Student Code of Conduct • Student Misconduct Procedures
Approval body	Director/CEO
Date effective	28 November 2014
Date of review	1 January 2017
Contact position	IT Manager
Policy No	ITP001
TRIM Record No	14/06480