

Policy name: Information and Communications Technology Policy

Approved: 25th November 2016

Revision 1 approved 10th March 2017

Revision 2 approved

Revision 3 approved by Trinity Academic Council 13th May 2020

1. Context

- 1.1 Information is a critical asset of the Royal Irish Academy of Music (hereinafter referred to as RIAM or the Academy). Accurate, timely, relevant and properly protected information is essential for the success of RIAM's academic and administrative activities. RIAM is committed to ensuring that all accesses to, uses of, and processing of this information is performed in a secure manner and that best practice standards are adopted during all information and communications technology (ICT) operations.
- 1.2 Technological information systems play a major role in supporting the day-to-day activities of RIAM. These information systems comprise all infrastructure, networks, hardware, databases and other software applications, which are used to manipulate, process, transport, or store information owned by RIAM.
- 1.3 Communication systems (including telephone, facsimile, email, broadband and web services) also play a vital role in helping staff to establish and maintain contact with RIAM's customers and stakeholders.
- 1.4 Information that RIAM or its contractual agents use in the course of conducting its business is an institutional resource. Although individuals and departments may have responsibility for creating and maintaining portions of RIAM information and records, the institution itself retains ownership of, and responsibility for this information.
- 1.5 RIAM recognises that failure to implement best practice standards and adequate security controls could potentially lead to (i) financial loss, (ii) irretrievable loss of important RIAM data, (iii) damage to RIAM's reputation, or (iv) legal consequences and GDPR . Thus RIAM has put in place measures to minimise the risk to RIAM from unauthorised modification, destruction or disclosure of data, whether accidental or deliberate.

2. Purpose

- 2.1 The ICT policy and the RIAM's procedures and structures will enable the institution to fulfil its responsibilities with regard to information security and ensure that a high level of service is provided to staff, students and other stakeholders.
- 2.2 This policy lays the foundation for a common understanding of information security at RIAM, based on the generally accepted principles of confidentiality, integrity and availability. Information access will be limited to authorised users; information will be kept up to date and protected against unauthorised modification; and information will be accessible when it is required by ensuring that systems are robust and fault tolerant.

- 2.2 The object of this policy is to define the security controls necessary to safeguard RIAM information and communications technology (ICT) resources and to ensure the confidentiality, integrity and availability of the information that is being stored and transmitted.
- 2.3 Information security management enables information to be shared while ensuring the protection of that information and its associated computer assets.
- 2.4 This policy outlines the framework that reflects RIAM's commitment to the management of risks associated with ICT assets and the reduction of ICT security incidents related to the confidentiality, integrity and availability of information housed in its ICT systems.

3. Scope

- 3.1 This policy applies to faculty, staff, students, and all others granted use of RIAM information or related assets ('service users') and defines their responsibility for the protection and appropriate use of RIAM information, applications, computer systems and networks.
- 3.2 Within the context of this policy, information refers to all information processed, stored, used or transmitted in any medium or form.
- 3.3 Information assets comprise databases and data files, customer information, student information, research information, system documentation, user manuals, training material, operational or support procedures, continuity plans, and archived information.
- 3.4 Software assets include application software, system software, bespoke software (specifically two SQL database applications, namely GO which caters for internal part-time and third level student administration, and LCEO which caters for the Local Centre external examination system).
- 3.5 Physical assets comprise the network (switches, links, connectors and cables); computer equipment (servers, Storage Area Network, virtual machines; workstations, laptops, processors, monitors, modems); communications equipment (e.g. routers, telephones, mobile phones, Wi-Fi access points), magnetic media (tapes and disks), other technical equipment (uninterruptible power supplies (UPS), air-conditioning units).
- 3.6 Communication and computing services (Internet, Wi-Fi, email, voicemail, file-sharing, printing, storage and backups).
- 3.7 The scope also includes the physical protection of all RIAM ICT assets.

4. Benefits

- 4.1 This policy provides a framework in which security threats to RIAM information and communication systems can be identified and managed on a risk basis.
- 4.2 It also establishes the terms of reference, which ensure uniform implementation of information and communication security controls throughout RIAM.

5. Principles

- 5.1 RIAM undertakes to ensure that the institution's information in any form, and related assets are created, used, communicated and maintained in a secure environment.

- 5.2 All RIAM information will be kept accurate and up-to-date and available for authorised use.
- 5.3 All RIAM computing facilities, programs, data, network and equipment will be monitored and kept adequately protected against loss, misuse or abuse.
- 5.4 Security measures must be implemented by all RIAM service users as part of the effective operation and support of ICT across the organisation and when used to communicate with the outside world.
- 5.5 All RIAM users must understand their own responsibilities for respecting the rights of individuals and protecting the confidentiality and integrity of the data they handle.
- 5.6 All RIAM service users must be aware of and fully comply with the relevant Irish and European Community legislation i.e. [Data Protection Act 2018](#) and [General Data Protection Regulation \(GDPR\)](#)
- 5.7 All RIAM service users must be aware of and fully comply with this ICT policy and the relevant supporting policies and procedures.
- 5.8 Successful implementation of this strategy can only be achieved if all service users cooperate by observing the highest standards of ethical, personal and professional conduct.

6. Policy

6.1 Custodianship and Protection

- 6.1.1 RIAM retains overall responsibility and ownership for all the institution's records, information and ICT assets.
- 6.1.2 Individuals and departments are tasked, as custodians, with creating and maintaining these assets.
- 6.1.3 Custodians of ICT assets are responsible for the protection, integrity and availability of those assets and for putting the appropriate controls and procedures in place.
- 6.1.4 Tangible assets are to be located in appropriately secure physical locations.
- 6.1.5 Controls and processes will be put in place to ensure assets are accurate, up-to- date and protected from unauthorised modification.

6.2 Access Control

- 6.2.1 Access controls for all RIAM ICT systems will be maintained at appropriate levels by ongoing proactive management.
- 6.2.2 Access to all RIAM ICT systems will use a secure log on process i.e. HEAnet's Edugate federated single sign on identity management system.
- 6.2.3 Staff will only be given access to those information systems that they are required to utilise in order to fulfil their duties. Line Managers must ensure that their staff have been adequately trained so that the integrity of the information systems can be maintained.

- 6.2.4 Where new staff members require access to the RIAM business network they will be assigned a network account in the Active Directory and a faculty licence for Office 365 by the system administrator.
- 6.2.5 New third level students will be given access to devices connected to the student network and allocated a student licence for Office 365.
- 6.2.6 Password for all RIAM systems are subject to the following rules:
- (i) No passwords are to be spoken, written, emailed, hinted at, shared, or in any way known to anyone other than the user involved. This includes teachers, supervisors and personal assistants.
 - (ii) No passwords are to be shared in order to "cover" for someone out of the office. Contact the ICT Manager at tech@riam.ie to request a temporary account if there are resources that need to be accessed.
 - (iii) Service users should not use proper names, address details, dates of birth, or any term that could easily be guessed by someone who is familiar with them.
 - (iv) Passwords should not to be displayed or concealed near workstations.
 - (v) Service users will be responsible for all activity conducted using their login details.
- 6.2.7 Passwords must meet the following criteria:
- (i) password should be at least six characters long;
 - (ii) password should contain 1 uppercase letter (i.e. A to Z);
 - (iii) password should contain 1 lowercase letter (i.e. a to z);
 - (iv) password should contain at least one number (i.e. between 2 and 9);
 - (v) password should contain at least one special character (e.g. %, &, *, !);
- Service users should change their passwords at regular intervals (every three months or whenever prompted by the system).
- 6.2.8 Service users should ensure that unattended equipment has appropriate protection by terminating active sessions once complete or by using a password protected screen saver prior to leaving the work station.
- 6.2.9 It is the policy of RIAM not to issue generic user accounts. Existing generic user accounts are to be reviewed and discontinued if no named user can be identified.
- 6.2.10 Whenever there is a change in business need, a user changes their role, or a user leaves RIAM, service user access rights will be adjusted appropriately and in a timely manner by the system administrator.
- 6.2.11 Where systems store data classified as 'confidential' or 'strictly confidential' additional steps will be taken to prevent unauthorised access. These may include encrypting the data and reviewing audit logs to monitor access to this data.

6.2.12 Two-factor authentication will be employed where non-RIAM users are allowed to access RIAM online services.

6.3 Software Protection

6.3.1 Only licensed software products should be installed on RIAM information systems and services to ensure that the RIAM conforms to all copyright laws.

6.3.2 The licensed products should only be installed by systems administrators.

6.3.3 The ICT Manager will audit installed software applications from time to time and may remove unauthorised or unlicensed software from information systems.

6.3.4 Unauthorised copying of software or the use of unauthorised products by service users may be grounds for disciplinary action, up to and including dismissal (for staff), and where appropriate, legal proceedings.

6.4 Email Service

6.4.1 RIAM recognizes that email is a fast, reliable and cost-effective method of delivering messages and documents and, in view of this, encourages its use. RIAM aims to provide an email facility that is capable of meeting the business needs of each stakeholder. However, this policy is not exhaustive. In situations that are not expressly governed therein, service users must ensure that their use of e-mail is at all times appropriate and consistent with their responsibilities towards RIAM. In case of any doubt, they should consult with their manager or the HR department.

6.4.2 Service users are required to behave in a professional and responsible manner whether accessing email from within the Academy or using RIAM resources over the Internet.

6.4.3 All emails sent will be identified by the username as coming from RIAM and service users should take care to uphold RIAM corporate values and good reputation.

6.4.4 It is recommended that all email messages sent from RIAM would automatically carry the following disclaimer:

The information in this email is confidential and may be legally privileged. It is intended solely for the addressee. Access to this email by anyone else is unauthorised. If you are not the intended recipient, any disclosure, copying, distribution or any action taken or omitted to be taken in reliance on it, is prohibited and may be unlawful. If you have received this electronic message in error, please notify the sender or the ICT Manager at tech@riam.ie.

This message has been swept by Anti-Virus software

6.4.5 Service users must adhere to laws on defamation, copyright, obscenity, fraud, discrimination and data protection when using email to communicate.

- 6.4.6 RIAM is not liable for any information sent by a user of the system in the event that the user chooses to send information in violation of this policy.
- 6.4.7 Commercial use, which is not connected to or approved by RIAM, is strictly prohibited.
- 6.4.8 Email is a business tool which should only be used for reasonable purposes. Reasonable use is defined as use that does not impair the system or impact negatively on user's job performance or on the work or reputation of the institution.
- 6.4.9 Reasonable personal use is permitted. However, service users are reminded that all information on the email system is the property of the RIAM and may be monitored. While RIAM does not routinely monitor the content of e-mail messages, it may, for computer maintenance and other purposes, analyse e-mails individually or collectively. Circumstances giving rise to such analysis include, but are not limited to:
- (i) investigations triggered by indications of misconduct;
 - (ii) the detection of computer viruses;
 - (iii) monitoring proper use;
 - (iv) the location of information required for business purposes;
 - (v) responding to legal or regulatory requirements;
 - (vi) fulfilment of obligations to customers, clients, third parties and relevant regulatory authorities.
- 6.4.10 The only personal email data that may be held in RIAM accounts is email information relating to RIAM business.
- 6.4.11 In particular, staff members who also have responsibility for communications on behalf of other organisations may not store other email data with RIAM email data, and, in general, unless explicit permission has been obtained from the Director, may not store email data relating to these other organisations on systems provided by the RIAM e.g. PCs, laptops, mobile phones, databases, etc.
- 6.4.12 It is inappropriate use of email to:
- (i) use someone else's ID to send mail;
 - (ii) use e-mail to circulate joke mail or chain letters, internally or externally;
 - (iii) use e-mail to harass or intimidate another person, broadcast unsolicited messages, or send unwanted mail;
 - (iv) communicate to another in any manner that could cause him or her distress, embarrassment, or cause unwarranted attention. There must be no personal attacks, inclusive of those based on gender, race, national origin, ethnicity, religion, disability, sexual orientation, or membership of the traveller community;
 - (v) use e-mail, or other system resources, to gain access to, or possession of, pornographic materials;

- (vi) accept/open electronic mail messages that might be harmful to RIAM's computing resources, or to information stored thereon;
- (vii) use vulgar, abusive, or hateful language;
- (viii) save, download, transmit or purposely view sexual, pornographic, racist, profane or other offensive material;
- (ix) download software, graphical or other forms of information for personal use;
- (x) produce advertising or listings for personal benefit;
- (xi) use the e-mail system to send mail that may be damaging to the organisation's corporate image;
- (xii) engage in any activity that is in competition with the commercial interests of the organisation;
- (xiii) subscribe to any contracts, unless you are authorised to do so within the terms of the organisation's policy on purchasing;
- (xiv) accept any material by e-mail that may give rise to a breach of the intellectual property rights of any outside party;
- (xv) engage in any other activity that does not comply with the principles presented above.

6.4.13 RIAM is committed to protecting its service users from the effects of inappropriate use of e-mail by others. If service users receive any offensive, unpleasant, harassing, or intimidating messages via e-mail, they should report this immediately. It is important that the sources of such e-mails are traced as quickly as possible. The message should be printed and kept for investigative purposes.

6.4.14 If any breach of this e-mail policy is observed and proven, then disciplinary action (for staff, up to and including dismissal) may be taken.

6.5 Direct Marketing

6.5.1 It is RIAM's intention to continue to use email to provide information, newsletters, updates, notices of events, invitations to concerts, solicitations for donations, etc., to its large and diverse community of stakeholders.

6.5.2 In compliance with [GDPR](#) when collecting personal information, including email addresses, RIAM must advise individuals what information is being collected, for what purposes, how long it will be retained, and how it can be corrected, updated or deleted by the individual.

6.5.3 Personal information collected for reasonable business purposes (e.g. processing an application for a Local Centre examination) that a person requests (and consents to) does not require additional explicit consent. Individuals providing information on behalf of others must confirm that appropriate consent has been obtained.

- 6.5.4 Personal information collected for communications or marketing purposes, outside of the normal RIAM reasonable business processes, requires explicit (opt-in) consent from individuals for each specific communications or marketing purpose. RIAM must carefully define these purposes and ensure that communications to individuals are consistent with the purposes for which explicit opt-in consent has been obtained. RIAM must record these consents.
- 6.5.5 RIAM has a large set of existing collected email addresses. It has been careful to ensure that implicit consent was obtained for the appropriate purposes, but must now establish a process to update these consents to explicit opt in consents.
- 6.5.6 RIAM will, over time, email all the individuals whose email addresses are on file, and
- (i) advise them of the purposes for which email addresses are currently being used;
 - (ii) advise them that email addresses currently on file will be deleted after [2] years on [date] (the Initial Retention Period); and
 - (iii) invite them to opt-in to one of more of a range of defined RIAM email communications.
 - (iv) Advise of ability to opt-out
- These consents will be recorded and will be used to ensure that thereafter the email addresses will only be used for the agreed purposes.
- 6.5.7 The wording of the email that will be sent out to stakeholders advising them of their rights and protection under GDPR will be approved by the ICT Steering Committee.
- 6.5.8 RIAM will delete all records of those individuals who have not provided their explicit consent for the various purposes at the end of the Initial Retention Period.
- 6.5.9 Users are expected to act ethically and responsibly in their use of emails for direct marketing purposes and to comply with the relevant national legislation available from the [Data Protection Commission](#) website.

6.6 Internet Usage

- 6.6.1 RIAM recognises that the Internet is an important business resource and aims to provide access to the Internet for its entire staff and student community subject to acceptance of this policy and abiding by its contents.
- 6.6.2 Internet access for business purposes in RIAM is available only via the RIAM infrastructure. Users wishing to connect a non-RIAM machine to the Internet via the RIAM network must seek authorisation from the ICT Manager.
- 6.6.3 RIAM third level students may access Internet through a secure Wi-Fi system.
- 6.6.4 All devices connected to the Internet must be equipped with the latest versions of anti-virus software, which has been both approved and supplied by RIAM. All forms of data received over the Internet will be immediately checked for viruses. All forms of data transmitted from RIAM over the Internet are virus checked. All security incidents involving Internet access must be reported to the ICT Manager.

- 6.6.5 Reasonable use is defined as use that does not impair RIAM systems or impact negatively on the service user's job performance or on the work or reputation of RIAM.
- 6.6.6 Commercial use, which is not connected to or approved by the RIAM, is strictly prohibited and will result in disciplinary procedures.
- 6.6.7 Service users are expected to act ethically and responsibly in their use of the Internet and to comply with the relevant national legislation, RIAM's regulations and codes of practice.
- 6.6.8 Service users must not post messages on newsgroups or chat areas that are likely to be considered abusive, offensive or inflammatory by others.
- 6.6.9 Software copyrights and license conditions must be observed. Only licensed files or software may be downloaded from the Internet.
- 6.6.10 Reasonable personal use is permitted. However, service users are reminded that all information stored on RIAM systems is the property of the Academy and can be monitored.
- 6.6.11 Due to the recent prevalence of threats such as viruses and spyware, service users are asked to be particularly vigilant when using the Internet. Non-reputable sites such as those offering free music or programme downloads must be avoided.
- 6.6.12 RIAM has restricted access to certain sites which have been blacklisted or which have been deemed to be unsuitable.
- 6.6.13 RIAM users are asked to avoid usage that would adversely affect productivity or consumes excessive network resources.
- 6.6.14 Service users are asked to refrain from posting, transferring, downloading, viewing or linking to material that is illegal, offensive, abusive, obscene, defamatory or threatening.
- 6.6.15 Service users should not violate copyright laws when downloading music files or images from the Internet.
- 6.6.16 Service users must not use the RIAM Internet connections (business and/or student networks) to scan or attack other individuals/devices/organisations.
- 6.6.17 Copyright and intellectual property rights of information service users may encounter on the internet must be respected at all times. This may require obtaining appropriate permission to make use of information and the giving of proper credit to the source of the information used for RIAM's purposes.
- 6.6.18 Material in which RIAM has a proprietary interest – such as software, documentation or other internal or confidential information – must not be transmitted, sold or otherwise transferred to any outside party, except in pursuance of RIAM's legitimate business interests. Any departure from this policy requires the written authorisation of the RIAM Secretary.

6.6.19 Misuse of internet facilities and services is prohibited. Access to the internet from a RIAM computer must never be used:

- (i) for personal gain or profit;
- (ii) to represent one's identity as someone else's;
- (iii) to post or download messages that will reflect poorly on RIAM's name and professional reputation;
- (iv) to advertise, or otherwise promote, unauthorised or illegal activities;
- (v) to promote or engage in any business activity that is in competition with the RIAM's business activities;
- (vi) to process the personal data of any person in a manner inconsistent with the data protection legislation requirements;

6.6.20 Non-compliance with the general principles and conditions of this internet policy may lead to disciplinary action, (for staff, up to and including dismissal).

6.7 Mobile Devices

6.7.1 Mobiles devices such as smartphone, laptops and tablet computers represent a significant risk to information security as they can easily become a conduit for unauthorised access to RIAM's data and ICT infrastructure, which could lead ultimately to data leakage and system infection.

6.7.2 Devices must be configured with a secure password.

6.7.3 With the exception of those devices managed by ICT, devices are not allowed to be connected directly to the internal business network.

6.7.4 Devices must be kept up to date with patches provided by the manufacturer.

6.7.5 RIAM users must not load pirated software or illegal content onto their devices.

6.7.6 Devices must not be connected to PCs which do not have up-to-date and enabled anti-virus/malware protection.

6.8 Physical Security

6.8.1 RIAM servers and storage area network (SAN) are located in a secure Communications Room with a protected power arrangement, uninterruptible power supply, and temperature-controlled environment.

6.8.2 Computer equipment is installed in office environments and should be locked when unattended.

6.8.3 Equipment that supports critical business activities are physically protected from security threats and environmental hazards to reduce the risk of damage, interference and unauthorised access.

- 6.8.4 Only authorised persons are admitted access to these areas and appropriate entry controls are implemented (e.g. intruder alarm system, CCTV cameras).
- 6.8.5 Cables carrying data or supporting information services are protected by using conduit, by avoiding routes through public areas and installing them underground where feasible.
- 6.8.6 Equipment is correctly maintained to ensure its continued availability and integrity and servicing is only performed by experienced personnel.
- 6.8.7 All data is completely erased from equipment and storage media prior to disposal.
- 6.8.8 Remote service users must abide by the following guidelines:
 - (i) personal computers should not be used for business activities if virus controls are not in place;
 - (ii) when travelling, equipment (and media) should not be left unattended in public places;
 - (iii) portable devices should be carried as hand luggage when travelling;
 - (iv) time-out protection should be applied;
 - (v) all mobile devices should have an appropriate form of access protection (e.g. passwords or encryption) applied to prevent unauthorised access to their contents;
 - (vi) passwords or other access tokens for RIAM systems should never be stored on mobile devices where they may be stolen and give the thief access to sensitive data;
 - (vii) security risks should be assessed and appropriate measures put into practice.
- 6.8.9 Physical security incidents can be defined as issues that affect the physical barriers and control procedures that are implemented to act as preventive measures and countermeasures against threats to resources and sensitive information.
 - (i) If a suspected physical security incident is identified the incident should be reported immediately giving as much detail as possible.
 - (ii) If the incident is clearly a significant breach of security the RIAM Secretary should be consulted.

6.9 Maintenance and Technical Vulnerability

Patch Management

- 6.9.1 Computer systems attached to the network must be updated accurately and timely with security protection mechanisms (patches) for known vulnerabilities and exploits to reduce or eliminate these vulnerabilities with limited impact to the business.
- 6.9.2 All security patches must be applied as soon as possible after their release and a log of the status of all patches will be recorded.

- 6.9.3 Monitoring software (panorama9) is used to check each device on the network and alert the system administrator when patches are due to be downloaded and installed.

Remote Access to Systems

- 6.9.4 Remote access is allowed via secure connections only.
- 6.9.5 VPN facilities are provided to RIAM staff for the purpose of remote systems administration and database access.
- 6.9.6 VPN connections are provided to authorised personnel who support applications remotely.

Anti-Virus Security

- 6.9.7 RIAM will provide means by which the latest version of site-licensed virus protection software can be downloaded and installed on all network devices.
- 6.9.8 Service users must ensure that they are running adequate and up-to-date anti-virus software at all times.
- 6.9.9 If any service user suspects that his/her machine has been infected with a virus, a complete virus scan should be performed.
- 6.9.10 If a machine is found to be behaving abnormally due to a possible viral infection this device will be disconnected from the network until deemed safe.
- 6.9.11 If a serious widespread virus attack occurs emergency procedures will be invoked. This will ensure immediate action by RIAM staff and students to ensure the safety of RIAM information resources through viral scan and disconnection.

6.10 *Change Management and Testing*

- 6.10.1 There is strict control over the implementation of changes to software installations.
- 6.10.2 Formal change control procedures are followed to ensure that security is not compromised and that formal agreement and approval for any change is obtained:
- (i) Authorisation of request for change.
 - (ii) Risk assessment of change.
 - (iii) User acceptance testing.
 - (iv) Relevant management sign-off.
 - (v) Information security sign-off.
 - (vi) Rollback procedures in the event that the new release failed.
 - (vii) Documentation of above steps.

6.11 Confidentiality and Privacy

6.11.1 RIAM and all RIAM staff, third level students and stakeholders are obliged to respect the rights of individuals and to protect confidential data. Attention is drawn in particular to the:

- (i) Code of Conduct.
- (ii) Breaches of the Code of Conduct.
- (iii) Legal requirements under the [Data Protection Act 2018](#) and [General Data Protection Regulation \(GDPR\)](#).

6.12 Business Continuity

6.12.1 Continuity of operations, plans and arrangements ensure that there are mechanisms in place to maintain, or quickly resume, essential services and operations within RIAM in the event of a catastrophic event (e.g. fire, flooding etc.) that would result in disruption of normal activities and services.

6.12.2 A disaster plan has been devised outlining the disaster recovery management procedures and processes to ensure the efficient and effective resumption of vital RIAM functions in the event of an unscheduled interruption:

- (i) review of RIAM systems, physical locations and current backup strategy;
- (ii) actions to be taken by members of staff in the event of systems failure or data loss;
- (iii) ongoing systems backup strategy;
- (iv) systems continuity testing procedures;
- (v) immediate actions to be taken.

6.12.3 Procedures for procuring replacement hardware or expanding web services have been agreed if disaster strikes.

6.12.4 The RIAM hybrid system is robust and reliable. An image of this system will be used to replicate the existing system as part of the recovery strategy.

6.12.5 All files stored in MS Azure cloud web services will be secure against attack.

6.12.6 There is a nightly backup taken of all essential files including two legacy SQL databases on the production virtual machine (RIAMSQL1) and all RIAM user files which have been saved to the RIAMFS1 virtual machine. Tapes are taken off site in order to have reliable backups in the event of a physical disaster such as fire or flooding. If files are deleted or become corrupt the original files can be restored from these tapes.

6.12.7 All RIAM staff must be prepared for a disaster event in which ICT equipment or data is destroyed by ensuring that they have taken a backup of all important data stored on equipment assigned to them, or that they have saved a copy of all of these files to their folders on the file server (RIAMFS1) which is backed up each night.

6.12.8 RIAM third level students are permitted to store files that created in class in their own individual home folders on a dedicated virtual machine, RIAMSTUFS1. Students are assigned secure RIAMTLS network login details to allow them to access computers in the Computer Room and the Library for this purpose. Students are also advised to save their own work to portable storage devices on a regular basis.

6.12.9 Service users should take care when using portable storage devices that they scan all such storage devices for viruses and malware before reusing them.

6.13 HEAnet Code of Behaviour

6.13.1 HEAnet is Ireland's National Education and Research Network, providing internet connectivity and associated ICT services to education and research and supplies enabling and enhancing services for RIAM in the pursuance of their official activities of instruction, research and development, and associated academic activities, and for administration in direct support of such use. RIAM has agreed that its staff and third level students will abide by HEAnet's code of behaviour.

6.13.2 According to this code of behaviour it is not permitted to use HEAnet services for any activity which purposely:

- (i) seeks to gain unauthorised access to the resources of member organisations;
- (ii) adversely affects the operation of HEAnet services or jeopardises the use or performance for other users;
- (iii) wastes resources (people, capacity, computer);
- (iv) destroys the integrity of computer-based information;
- (v) compromises the privacy of users;
- (vi) creates or transmits (other than for properly supervised and lawful research purposes) any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or material;
- (vii) creates or transmits defamatory material;
- (viii) transmits material in such a way as to infringe the copyright of another person or organisation;
- (ix) transmits unsolicited commercial or advertising material;
- (x) causes offence or discriminates on grounds of race, creed or sex. In particular, compliance with the [Employment Equality Act 1998](#), [Equal Status Act 2000](#) and the [Equality Act 2004](#) is required – including any amendments to said acts;
- (xi) conflicts with practices as laid down from time to time by the Board contravenes the law of the State (in particular, but not exclusively, the [Data Protection Act 2018](#) and the [Criminal Damages Act \(1991\)](#)).

7. Procedures

- 7.1 Compliance with this policy is mandatory and will be deemed to be part of the contract of employment for staff and third parties. Each user must understand his/her role and responsibilities regarding information security issues, and protecting RIAM's information assets.
- 7.2 Failure to adhere and comply with this ICT policy that results in the compromise of RIAM information confidentiality, integrity and/or availability may result in disciplinary action (for staff, up to and including dismissal) and possible prosecution under applicable legislation.
- 7.3 Any compromise or suspected compromise of this policy must be reported as specified in the Code of Conduct.
- 7.4 An ICT security Incident is defined as any activity that harms or represents a serious threat to the whole or part of RIAM's computer, telephone and network-based resources such that there is an absence of service, inhibition of functioning systems. This includes unauthorised access or changes to, or theft of hardware, firmware, software or data, or a crime or natural disaster that destroys access to or control of these resources. It also includes the use of ICT resources in a manner that constitutes a criminal act.
- 7.5 Users of information systems are required to note and report any observed or suspected security weaknesses in, or threats to, systems and services. Such weaknesses or threats should be treated as security incidents, and be reported promptly to the ICT Manager.
- 7.6 All ICT incidents must be reported without delay to the ICT Manager, to the Line Manager or Senior Management as appropriate.
- 7.7 Evidence relating to a suspected data security breach should be recorded and notified to the Data Controller and Data Protection Officer and appropriate remedial action taken immediately.
- 7.8 Security incidents reported to the ICT Manager will be subject to appropriate internal procedures. Where it is deemed appropriate files may be deleted to minimise the risk of propagation or the network may be isolated to maintain its integrity.
- 7.9 All employees should be made aware that evidence of information security incidents may be formally recorded and retained.
- 7.10 Wherever possible, the RIAM will undertake to prevent incidents by monitoring and scanning its own network for anomalies, and developing clear protection procedures for the configuration of its ICT resources.
- 7.11 It is acceptable to open emails and attachments from trusted sources. However if an email is received from an unrecognised sender or with a non-standard attachment type, the recipient should not open the email but instead contact the ICT Manager immediately at tech@riam.ie.
- 7.12 It is acceptable to open attachment using standard file formats e.g. MS Word, MS Excel, etc. In order to maintain the integrity of ICT systems, staff members are urged to contact the ICT Manager should it be necessary to open any non-standard file formats.

- 7.13 Service users are asked to display common sense and courtesy when handling emails, as any action that adversely affects ICT systems will impact upon the business/educational needs of all service users in RIAM.
- 7.14 RIAM users must not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist. RIAM reserves the right to block or monitor access to such material.
- 7.15 These procedures will be reviewed periodically to adjust processes, identify new risks and remediation methods.

8. Responsibility

- 8.1 The responsibility for protecting ICT systems and information rests with all staff, third level students and third parties who use or have involvement with the systems. Both the RIAM ICT user community and ICT services have responsibilities to ensure compliance with this policy.
- 8.2 The RIAM Senior Management team has overall responsibility for the RIAM ICT policy to protect the assets of the institution. Appropriate procedures must be in place together with management, monitoring and review processes to ensure that policies are implemented, adhered to and kept up-to-date.
- 8.3 The ICT Steering Committee oversees the ICT infrastructure, database systems and assets, makes recommendations to Senior Management, reports on ICT security matters and ensures that policies are implemented in order to avoid breaches of legal, statutory, regulatory, contract or privacy obligations.
- 8.4 The ICT Manager plays a key role in the implementation of the ICT Policy and has responsibility for monitoring the RIAM network infrastructure, including all hardware and communication links, reporting any audit issues that may be identified in relation to these items, and providing advice and assistance to end users.

9. Legislation and Regulation

- 9.1 [Copyright and Related Rights Act 2000, 2004 and 2007.](#)
- 9.2 [Data Protection Act 2018.](#)
- 9.3 [Child Trafficking and Pornography Act 1998.](#)
- 9.4 [Child Trafficking and Pornography \(Amendment\) Act 2004.](#)
- 9.5 [Criminal Damages Act 1991.](#)
- 9.5 [Defamation Act 2009.](#)
- 9.6 [Employment Equality Act 1998.](#)
- 9.7 [Equal Status Act 2000.](#)
- 9.8 [Equality Act 2004.](#)
- 9.9 [Prohibition of Incitement to Hatred Act 1989.](#)

- 9.10 [Qualifications and Quality Assurance \(Education and Training\) Act 2012.](#)
- 9.11 [Standards and Guidelines for Quality Assurance in the European Higher Education Area \(2005\).](#)
- 9.12 [Code of Practice for Provision of Education and Training to International Learners \(2015\).](#)
- 9.13 [National Framework of Qualifications \(NFQ\).](#)
- 9.14 [General Data Protection Regulation \(GDPR\) 2018.](#)
- 9.15 Rules for Electronic and Direct Marketing at [Data Protection Commission.](#)

10. Related Documents

- 10.1 Staff Disciplinary Policy.
- 10.2 Staff Grievance and Mediation Policy.
- 10.2 Student Code of Conduct.

11. Review

- 11.1 This policy will be reviewed on a three year cycle, or as required to take into account changes in the law and the experience of the policy in practice.

12. Document Control

Approved by Board of Studies 25th November 2016.
Revision 1 approved by Board of Studies 10th March 2017.
Revision 2 approved.
Revision 3 approved by Trinity Academic Council 13th May 2020.
Next review: Academic year 2020/21.

Appendix: Acknowledgment of the RIAM ICT Policy

This form is used to acknowledge receipt of, and compliance with, the RIAM ICT Policy.

Procedure

Complete the following steps:

1. Read the ICT policy
2. Sign and date in the spaces provided below
3. Return this page to the ICT Manager/Librarian/Administrative Officer

Your signature indicates that you have read the RIAM ICT policy. Signing this document does not mean that you agree with each and every provision of the policy. However, it does mean that you will abide by the regulations set forth in the above policy. By signing below, I agree to the following terms:

1. I have received and read a copy of the RIAM ICT policy, and I understand the same.
2. I agree that, if I leave RIAM for any reason, I shall immediately return to the company any equipment that I may have received from the company that is either in my possession or otherwise directly or indirectly under my control and will discontinue the use of any communication device or user ID that was provided.
3. I agree that I will adhere to the regulations set forth in the ICT policy.

Employee/Student signature:

Employee/Student name (printed):

Date: