Computer and Information Technology Policy

1. Background

This Policy provides all staff, students and third parties of ISA with guidelines for the secure use of ISA's Computer and Information Technology (CIT) resources.

ISA's CIT resources facilitate ISA business systems and its communications. These resources are essential tools provided to staff and students to meet its responsibilities in providing cutting edge education and training. ISA encourages the use of its CIT resources for contractors and visitors where required.

This policy applies to all staff and students as well as all authorised third parties including visiting staff, guests, contractors and other users of ISA's CIT resources, onsite or externally.

2. Definitions

Computer & Information Technology (CIT): CIT includes all network systems, phone (including mobile) systems, desktop and laptop computers, software, and internal and external connections to the Internet via the ISA infrastructure. It extends to all current, emerging and future technologies.

Users: ISA staff including casual staff; all ISA students including all students enrolled in full time courses and all students enrolled in short courses; all visitors, guests and contractors to ISA.

3. Policy

ISA provides CIT resources to Authorised Users for the purposes of education, training, teaching, production and creative work, events and exhibition and to conduct all other business and communications. All Authorised Users will use ISA's CIT resources for these purposes and exercise their use in a legal, ethical and responsible manner and according to this policy.

The following principles apply to this policy:

- ISA requires all Users of its CIT resources to abide by the ISA Code of Conduct and to use its CIT resources in a legal, ethical and responsible way.
- ISA takes all precautions to secure its CIT resources and to protect the privacy of individuals and confidentiality of material as appropriate. Users need to be aware that the normal course of securing the system includes but is not limited to actions such as backup, logging of activity and monitoring general usage.
- ISA may disclose electronic communications, records and other transactions to the appropriate authorities if legally required to do so.

3.1 Conditions of Use

- The primary User of a computer is considered to be a custodian of the equipment. Computer equipment must not be moved or relocated without the approval of the Facility Manager. If the equipment has been damaged, lost, stolen, borrowed or is otherwise unavailable for normal activities, the custodian must promptly inform the Facility Manager or an ISA staff member.
- Files and software may only be loaded onto an ISA computer systems in consultation with the Facility Manager. Only users with Administration privileges may load software themselves
- Users must not use ISA CIT resources;

  a) for private business activities, however, incidental personal use of CIT resources is permissible so long as:
     - it only uses a trivial amount of resources;
     - it does not interfere with productivity;
     - it does not pre-empt any ISA business activities; and
     - it is not used to make political, religious or other similar statements to any external recipient or organisation including but not limited to governments, the press and charities.

  b) to solicit, collect, use, disclose, alter or store personal information in any way that breaches the Privacy Act 1988.

  c) to access, transfer or store, or reproduce, copy, communicate publicly or otherwise use, any material without an appropriate license if to do so would or is likely to contravene the Copyright Act, 1968. Applicable material may include, but is not limited to, software, images, artistic work, live pictures, computer games, film, music and video.

  d) to access pornographic material. Transmission is not permitted under any circumstance.

  e) in inappropriate ways, which are likely to corrupt, damage or destroy data, software or hardware, either belonging to ISA or to anyone else, whether inside or outside the network. Users may only delete and alter data as required by their authorised School activities

  f) to acquire, possess, trade or use hardware or software tools that could be used to evaluate or compromise ISA's information systems and networks or allow unauthorised access to ISA's systems and information. This includes, but is not limited to, bridging ISA networks to the Internet or other external network and exposing systems or data through servers or other tools.

  g) to copy software provided by ISA without written permission from the Facility Manager

  h) in a harassing, discriminatory, abusive, rude, insulting, threatening, obscene or otherwise inappropriate or illegal manner.

- All files downloaded from non-ISA sources via the Internet or received via the ISA email system must be screened with virus detection software prior to being used.
- Computer systems provided by ISA must not be altered or added to in any way without the prior approval of the Facility Manager.
- ISA reserves the right to revoke CIT privileges of any User at any time.
- ISA reserves the right to remove any material it views as offensive or potentially illegal from its CIT systems.

- ISA reserves the right to delete, summarise or edit any information stored on ISA's CIT resources.

3.2 Security, Privacy & Confidentiality

- ISA takes all reasonable steps to secure its CIT resources and ensure all confidential and personal information stored in its CIT resources are electronically safeguarded as required by the Privacy Act 1988 and in accordance with best practice. However it cannot guarantee the protection of such confidential and personal information.
- All files, communications and other data transmitted and stored on ISA CIT resources are regarded as ISA records, including any data resulting from permitted incidental personal use.
- Users must take reasonable efforts to ensure that every electronic document created by them and designated as 'Confidential' displays the Confidential marking on the first screen shown to the recipient. All hardcopy computer output generated by a User and designated as Confidential must be marked Confidential. All computer-readable storage media containing Confidential information must have a Confidential designation on its external label. When not in use, this media must be stored in a locked safe, draw or cupboard, or a similarly secured location.
- Users in possession of ISA computers including laptops, notebooks, smartphones and other portable computers that contain Confidential Information must not leave these computers unattended at any time unless the Confidential Information is stored in encrypted form or its access can only be gained using a password.

3.3 Monitoring

- ISA reserves the right at any time and without notice to monitor, access, retrieve, copy, read, and/or disclose any files, communications or system information stored or transmitted using ISA CIT resources.
- All files and messages stored on ISA CIT systems are routinely copied to tape, disk and other storage media. Information stored on ISA systems - even if it has been specifically deleted - is often recoverable at a later date to be examined and where relevant, subpoenaed.
- Access to all websites is recorded in the proxy log generated by the proxy server and all information technology actions are routinely logged.

3.4 Breaches

- All suspect policy violations, system intrusions, virus infestations, and other conditions that might jeopardise ISA data and CIT systems must be immediately reported to the Facility Manager. These violations, intrusions, infestations and other conditions include but are not limited to:
  - Suspicion that sensitive ISA information is, or is suspected of being, lost or disclosed to or used by unauthorised parties.
  - Belief that password or other system access control mechanisms are, or are suspected of being, lost, stolen or disclosed.
  - Unusual systems behaviour such as missing files, frequent system crashes, misrouted messages that indicate a potential virus or security problem.
- Cases of serious, deliberate, and/or criminal breach will be referred to external authorities and may result in civil or criminal proceedings.

- If a request for information held on ISA computers is received from an external authority in regard to cases of potentially serious, deliberate, and/or criminal breach, the request must be forwarded to the Managing Director.
- Where Users are found to be in breach of this policy, penalties will depend upon the type and severity of the breach. Penalties may range from the loss or restriction of access, to formal disciplinary action.
- If a staff member has a suspicion that this policy is being breached through fraudulent activity they should refer the matter to the Facility Manager, Managing Director or relevant authorities.

4. Publication and Version Control

Staff and students are advised of this policy through publication on the ISA's website

Version	Amendments	Approval	Date Approved
2	Technical Manager changed to Facility Manager	Facility Manager	14/12/15