Cork Institute of Technology

Computer Systems Acceptable Usage Policy

Date of this revision: 09/10/2009

Document History

Document Location

This is a snapshot of an on-line document. Paper copies are valid only on the day they are printed. Refer to the author if you are in any doubt about the currency of this document.

Revision History

Date of this revision: 09/10/2009	Date of next revision: N/A

Revision Number	Revision Date	Summary of Changes	Changes marked
0.1	09/02/08	Initial Computer Systems Acceptable Usage Policy	
2.0	19/08/09	Revised Computer Systems Acceptable Usage Policy, GC, Submitted to O'Flynn Exhams for legal review	
3.0	30/09/09	Returned copy of CUP, post legal review (as discussed with TUI)	
4.0	09/10/09	Revised CUP incorporating certain changes required by TUI including Protocol for Dealing with Breaches of the CUP	
4.1	10/11/09	Acknowledged principle of Academic Freedom in general and, specifically, in the context of monitoring under Section 2.6. Amended Protocol to expand on circumstances when Staff will not be notified of a suspected breach of Policy.	

Approvals

This document requires following approvals –

Name	Title	Date
Gerard Culley	IT manager	30/11/09
Tony Collins	HR Manager	30/11/09
Paul Gallagher	Secretary/Financial Controller	30/11/09
Dr. Brendan Murphy	President of CIT	30/11/09
Governing Body	Chair of Governing Body	3/12/09

TABLE OF CONTENTS

1 Introduction and Purpose

1.1 *Background*

Cork Institute of Technology, including its constituent colleges the Crawford College of Art and Design, the Cork School of Music and the National Maritime College of Ireland, ("CIT" or "Institute") is recognised and respected as a progressive educational institution, in the local region and beyond. The Institute has consistently shown leadership in education within the State and, in particular, in the Institute of Technology sector. It has long been characterised by its talented and diverse student body, its highly sought after graduates, and its talented and committed staff.

Information technology ("IT") is a key service on which CIT's Staff and students depend and more importantly the security of that information. IT Security is now a critical core responsibility of the Institute. A lack of robust IT Security and an associated policy can lead to reputational and other damage and loss to the Institute, its Staff and students as demonstrated by numerous high profile security breaches in other sectors in recent years.

In light of these factors, it is clear that CIT requires a robust IT Security and Acceptable Usage Policy, one that protects the Institute's reputation and also protects Staff and students of the Institute. In devising this Policy, the management of CIT have utilised the previous Computer Systems Acceptable Usage Policy (February 2008) and made the following changes.

- We have modified the structure and layout of the document to make it easier to read, to remove repetition and overall have made it more consistent and professional.
- We have enhanced the responsibilities of the Institute in protecting data and relevant rights to privacy.
- We have referenced the relevant legal frameworks and guidelines which inform this Policy.
- We have transferred all guidelines and operational procedures to the appendices to this Policy. While failure to follow such guidelines and procedures will not in itself necessarily constitute a violation of this Policy, the guidelines and procedures may be taken into account when investigating any suspected violation of the Policy.

1.2 *Glossary of Terms*

In this Policy:

- "IT Security" means the prevention of breaches or compromises of the confidentiality, integrity and availability of CIT Resources and CIT Data which is entered, processed or transformed and recorded using electronic means;
- "IT Acceptable Usage" means the appropriate and proper use of CIT Resources and CIT Data and which does not result in reputational or other damage or loss to CIT;
- "CIT Data" means any electronic information stored, processed or transmitted using CIT Resources;
- "Confidential Data" means any CIT Data which is expressly described or marked as confidential or which is manifestly of a confidential nature and includes any information which CIT and/or Staff have received or shall receive from a third party subject to a duty on the part of CIT and/or Staff to safeguard the confidentiality of such information and/or to use such information only for certain specified purposes;
- "CIT Resources" (also referred to as "Resources" in this policy) means all IT systems owned, held under licence or otherwise controlled by CIT including but without limitation to;
    - Workstations including desktop machines and laptops
    - Servers
    - Network media such as routers and wireless routers
    - Printers
    - iPhones and other portable devices
    - USB memory devices
    - All other media and devices provided by CIT

- "Personal Data" has the meaning given to the term "personal data" in the Data Protection Acts 1988-2003;
- "Staff" means all full-time and part-time employees, contractors, visitors, and postgraduates of CIT.

1.3 *Scope and Authority*

This Policy governs IT Security and IT Acceptable Usage of:

- CIT Data
- CIT Resources

This Policy has been developed and approved by the Institute Executive Board (IEB) and forms part of Institute regulations. CIT is committed to developing a training program to accompany this Policy and help ensure that Staff can comply with the Policy to the greatest extent possible.

By logging on to and/or using any CIT Resource whether directly or by remote access or other means, Staff shall be deemed to have agreed to be bound by the terms of this Policy (as amended from time to time) and to have provided their consent to the processing of their Personal Data as set out in this Policy.

Staff who access CIT Resources and CIT Data using resources or equipment other than CIT Resources, either through remote access or other means, accept by doing so that they are fully responsible for their actions and for the security and appropriate usage of any CIT Data or resources accessed.

All CIT Data is deemed to be the property of the Institute for the purposes of assessing and monitoring compliance by Staff with this Policy. This is without prejudice to the rights of Staff concerning their Personal Data pursuant to the Data Protection Acts 1988-2003.

The Institute provides CIT Resources for Staff to use to support the normal activities of the Institute, in particular for educational, research and administrative purposes. While the Institute respects the right to privacy of Staff, this is not absolute, and in the interest of preserving the good reputation of the Institute, avoiding damage and loss to the Institute, and in providing a productive, healthy working environment for Staff the Institute reserves the right to access any data held on CIT Resources.

Nothing in this Policy seeks to limit the principle of academic freedom as set out in the Institutes of Technology Acts 1992 to 2006.

1.4 *Roles and Responsibilities*

The following shall have the following roles and responsibilities in relation to this Policy:

Institute Executive Board (IEB):

- To review and approve the Policy.

Secretary / Financial Controller (or nominated Chief Information Officer Representative):

- To ensure the Policy is reviewed and approved by IEB..
- To liaise with Human Resources (HR) on information received in relation to potential breaches of the Policy.

IT Manager:

- To define and implement standards and procedures which enforce the Policy
- To monitor compliance with the Policy
- To inform the Secretary / Financial Controller of suspected non compliance and/or suspected breaches of the Policy.

HR:

- To follow relevant and agreed disciplinary procedures when HR is informed of a potential breach of the Policy.
- To manage the disciplinary process.

If you have any queries on the contents of this Policy, please contact the IT Manager.

2 IT Security

CIT acknowledges that it is responsible for overall IT Security within the Institute. However, providing a secure, efficient and reliable computing and network system depends on the cooperation of all users, including Staff, who are required to use CIT Resources in a responsible manner, respecting the integrity of CIT Resources and CIT Data to which they have access.

It is the responsibility of all members of Staff to familiarise themselves with the steps outlined in this Policy and to conduct their activities accordingly. While minor or isolated incidences of failure to follow the steps outlined in this section 2 will not generally be treated as a violation of this Policy, repeated, wilful or reckless disregard for those steps may be treated as such and may be dealt with in accordance with section 6.

The aim of the Policy as it relates to IT Security is to ensure the three key principles of security are implemented in CIT - these are confidentiality, integrity and availability.

- ***Confidentiality:*** Confidential Data remains confidential and access to such data is on a needs-only basis.
- ***Integrity:*** CIT Data and CIT Resources are and remain accurate and reliable in so far as is practicable.
- ***Availability:*** CIT Resources are available for use in so far as is practicable.

In order to implement the above framework the Policy is set out under the following sub headings which form the building blocks for good IT Security practice:

- *Authorisation*
- *Administration*
- *Identification and Authentication*
- *Availability*
- *Auditability*
- *Monitoring*

2.1 *Authorisation*

Access to CIT Resources and CIT Data is provided on a **needs-only** basis, that is, Staff are given the minimum level of access that is deemed necessary for the performance of their particular job or role.

All members of Staff who access Personal Data must ensure that such data is processed in accordance with the Data Protection Acts 1988-2003. Further detail in relation to the requirements of that legislation is provided in Section 4 of this Policy and in CIT's "Data Protection Policy". To help ensure, in so far as practicable, that all relevant data protection legislation, guidelines and procedures are complied with the following needs to be adhered to in relation to data transmission, data storage and data disposal:

2.1.1 Data Transmission

CIT Data is not to be transmitted without adequate precautions being taken to ensure that only the intended recipient can access such data. Such precautions include [●]

2.1.2 Data Storage, Use and Back-Up

All CIT Data is to be stored securely and for no longer than is necessary. In all cases, Confidential Data is to be stored on CIT Resources and not on personal desktops, laptops and other media (USB keys, CDs, etc.) except where this is not practicable. Where CIT Data is exceptionally stored on personal desktops, laptops and other media, these devices shall use strong encryption techniques such as [●] to protect the data.

Staff using CIT Resources shall ensure that all CIT Data is backed-up. Backing-up should be done using one or a combination of the following methods:

- Backing-up to a local device separate from the primary data store e.g. Zip Drive, CD-Rom, Memory Stick, or other secondary device; and/or
- Regular saving or copying of CIT Data to a networked server which is then properly backed up by IT Manager. The usual network location would be the Staff member's home directory.

Any action taken to back-up CIT Data should not compromise the secure storage of such data. Further details and guidance in this regard can be obtained from the Services Desk and/or from individual departments where servers are not under the control of the IT Department.

2.1.3 Data Disposal

All hardware used for the storage of CIT Data is to be wiped of data and securely destroyed once it is no longer to be used.

When tapes and other secondary storage devices reach the end of their useful life they are to be purged of CIT Data and securely destroyed.

2.2 *Administration*

Access to CIT Data is administered, in certain instances, on a faculty and functional area basis. Individual faculties and functional areas within CIT may have specific procedures in place in relation to administering access to CIT Data. Such procedures may, for example, require Staff to obtain the approval of specified persons before accessing CIT Data. Staff shall be required to comply with such procedures provided that such compliance does not conflict with the terms of this Policy.

Administration procedures may also seek to address:

- User account creation
- User account amendment
- User account removal/deletion
- Periodic user account review

It is intended that there will be at least an annual review of system user listings focusing on the validity and appropriateness of access levels.

2.3 *Identification and Authentication*

The majority of Institute systems use user-names to identify Staff and passwords for authentication purposes. As passwords are the main authentication mechanism, this Policy provides minimum requirements in relation to passwords. In addition, smart cards are now being used as an additional layer of authentication for identifying Staff and accordingly this Policy also provides minimum requirements in relation to smart cards.

2.3.1 Password Use

All Staff, including administrators, are required to use robust passwords. For more information in connection with user accounts Staff should refer to the "Password Guidance" document in Appendix 1.

2.3.2 Password Protection

All Staff are required to protect their passwords. For more information Staff should refer to the "Password Guidance" document in Appendix 1.

If an account or password is suspected to have been compromised, please report the incident immediately to the Services Desk and change all passwords.

2.3.3 Smart Cards

It is the responsibility of Staff to protect their smart card and in this regard, smart cards shall not be provided to or shared with other persons.

If a smart card is missing and/or has been taken by another person to whom it is not assigned, please report the incident immediately to the Services Desk (see Section 6).

2.4 *Availability*

In order to ensure that CIT Data and CIT Resources are available when required, there are three main layers of controls:

- Prevention of CIT Data loss through CIT Data back-up (see section 2.1.2).
- Prevention of system downtime and/or unauthorised CIT Data access and amendment through anti-virus protection.
- Ability to respond to events which prevent CIT Data/CIT Resource access through disaster recovery planning.

2.4.1 Anti-virus

All devices that connect to CIT Resources must employ adequate and up-to-date anti-virus software. All CIT Resources must run the Institute's anti-virus solution as updated. CIT reserve the right to disconnect any machine, device or resource that is deemed not to have adequate levels of anti-virus protection.

For more information Staff should refer to the "Anti-virus Guidance" document in Appendix 1.

2.5 *Auditability*

An appropriate audit trail of the creation, amendment and deletion of CIT Data is maintained by CIT. This is particularly important in relation to the following:

- data including details on Staff, students and suppliers.
- data including inward fee payments, outward supplier payments, and payroll transactions.
- CIT Resource usage data.

CIT may log any required CIT Data concerning systems access, including data relating to unauthorised access attempts which may warrant investigation.

2.6 *Monitoring*

CIT respects the right to privacy of Staff. However, this right must be balanced against CIT's legitimate right to protect its interests. CIT is committed to ensuring robust IT Security and to protecting Staff, students and third parties from illegal or damaging actions carried out by groups and/or individuals either knowingly or unknowingly. To achieve its aims in this regard, CIT reserves the right to monitor all CIT Resources and CIT Data. Any monitoring of CIT Data and/or CIT Resources may be random or selective depending on circumstances at that time.

CIT monitoring takes the following three forms;

- Ongoing monitoring: using logs on CIT Resources such as those produced by firewalls and domain controllers.
- Proactive monitoring: using LANGuardian to monitor and validate network traffic on an ongoing basis and other software to combat the risk of viruses and other security breaches.
- Periodic content scanning: Conducted on a periodic basis (usually annually), the purpose of this scanning is to ensure that CIT Data and CIT Resources are being used in accordance with this Policy. CIT seeks to achieve this purpose without being unnecessarily intrusive. Accordingly, the software used by CIT for carrying out content scanning is primarily concerned with detecting inappropriate or illegal images and files. Content scanning does not typically involve CIT reading the content of individual communications. Please refer to the "Guidance on the Performance of Periodic Content Scanning" document in Appendix 1 and CIT's "Protocol For Dealing With the Results of Periodic Content Scanning" for more information in relation to content scanning.

All monitoring authorised by the Institute is designed to be proportionate so as to protect CIT Data and/or CIT Resources, as the case may be, and to reduce the risk of reputational and/or loss or damage to CIT and/or inappropriate/illegal use of CIT Data and CIT Resources, while taking into account the legitimate right to privacy of Staff.

When reviewing the results of any monitoring conducted in accordance with this Section 2.6., CIT will bear in mind that academic member's of Staff may be in possession of certain material for legitimate teaching and/or research purposes. Academic members of Staff will not be disadvantaged or subjected to less favourable treatment as a result of CIT monitoring provided they exercise their academic freedom within the law and can demonstrate that their teachings, research or qualifications are relevant to material detected and results revealed by CIT monitoring.

3 IT Acceptable Usage

Staff are afforded access to CIT Resources to assist them in carrying out their duties for the Institute. CIT Resources shall be used primarily for educational, research and administrative purposes. A limited amount of personal usage of CIT Resources is acceptable provided it:

- Does not consume more than a trivial amount of resources.
- Does not interfere with department or Staff productivity (this is at the discretion of the Head of the relevant Department/Faculty).
- Is not for private commercial gain.
- Does not prevent others with genuine Institute-related needs from accessing CIT Resources.
- Does not involve inappropriate conduct.
- Does not involve any illegal, inappropriate or unethical activities.

Staff shall observe the following general IT Acceptable Usage rules for all CIT Resources:

- Respect the legal protections of data and software provided by copyright and licences.
- Do not illegally transmit another's intellectual property or other proprietary information.
- Do not remove any copyright, trademark or other notice of proprietary rights.
- Do not send, obtain, upload, download, store, transmit, disseminate and/or distribute communications, material or images prohibited by law or communications, material or images of a pornographic, obscene, indecent, abusive, threatening, harassing, libellous, racist or extreme political nature, and/or which may be offensive to other members of Staff or harmful to minors, or which incite/promote violence, hatred or any illegal or inappropriate activity.
- Do not send or forward group/chain mails or generate spam.
- Do not intentionally distribute viruses, worms, defects, Trojan horses, corrupted files, hoaxes, or any other items of a destructive or deceptive nature.
- Do not manipulate to functioning or appearance of any web page or email or the content thereof.
- Do not use CIT Resources to make unauthorised entry into or access to any other computer, IT system or network.
- Do not conduct or forward pyramid schemes or other schemes of a similar nature.
- Do not disrupt or interfere with other computers or network users, services, or equipment. Intentional disruption of the operation of computer systems and networks is a crime.
- Do not represent yourself as another person or otherwise misrepresent yourself or the source of any communication.
- Do not use CIT Resources to violate the legal rights of others.
- Do not use CIT Resources for any illegal or unauthorised commercial purpose.
- Do not modify, adapt, translate or reverse engineer any aspect of CIT Data or CIT Resources.
- Do not engage in any illegal peer-to-peer file sharing.

In order to protect the interests of Staff, students and the Institute, system based controls have been implemented to prevent inappropriate usage. It is a violation of this Policy to intentionally circumvent these controls.

It is also important to re-iterate that CIT Data is only to be used for legitimate CIT business and is not to be shared with any other persons or organisations.

Please note the following-

- Internet and email activity is monitored and logged.
- All electronic mail coming into or leaving the Institute is scanned for viruses.
- You should not forward electronic mail messages to others, particularly newsgroups or mailing lists, without the permission of the originator.
- Delivery or receipt of email to external organizations cannot be guaranteed by the Institute due to the nature of email and the internet.

By using CIT Resources, Staff consent to all such monitoring, logging and scanning.

4 *Data Protection Acts 1988 to 2003 & Other Relevant Legislation*

4.1 *Data Protection Acts 1988 to 2003*

The use by Staff and monitoring by CIT of CIT Resources may involve the processing of Personal Data. CIT is committed to complying with its obligations thereunder, including the principles that Personal Data:

(a) shall be obtained and processed fairly;
(b) shall be kept only for one or more specified and lawful purposes;
(c) shall not be used or disclosed in any manner incompatible with that purpose or those purposes;
(d) shall be kept safe and secure;
(e) shall be accurate and kept up-to-date;
(f) shall be adequate, relevant and not excessive;
(g) shall not be retained for longer than is necessary for the purpose or purposes;
(h) shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of Personal Data; and
(i) appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data.

CIT strives to meet its legal obligations under the Data Protection Acts 1988 to 2003 through appropriate management and controls.

Staff shall comply with the provisions of the Data Protection Acts 1988 to 2003 and should familiarise themselves with their obligations in this regard. The Office of the Data Protection Commissioner has made available information and guidance booklets which Staff may access through the following address: http://www.dataprotection.ie/docs/Home/4.htm

By logging on and/or using CIT Resources, Staff shall be deemed to have consented in connection with such use to:

(a) the processing of their Personal Data by CIT and its audit partners in accordance with relevant law; and
(b) the transfer of their Personal Data outside the European Union.

4.2 Other Relevant Legislation

In addition to the Data Protection Acts 1988 to 2003, CIT is committed to ensuring compliance by Staff with Irish and EU law in connection with Staff use of CIT Resources and CIT Data, including but not limited to:

- The Child Trafficking and Pornography Acts 1998 to 2004;
- The Copyright and Related Rights Act 2000;
- The Criminal Damage Act 1991;
- The Electronic Commerce Act 2000 and the EC (Directive 2000/31) Regulations 2003 (S.I. No. 68 of 2003);
- The Freedom of Information Acts 1997-2003;
- The Non-Fatal Offences Against the Person Act 1997;
- The Prohibition of Incitement to Hatred Act 1989.

Staff shall not breach Irish or EU Law, including but not limited to the foregoing, in their access to and use of CIT Resources and CIT Data. Failure by Staff to comply with their obligations under all relevant laws in connection with their use of CIT Resources and/or CIT Data may lead to criminal prosecution and/or appropriate action being taken by CIT under its disciplinary procedures, including summary dismissal for gross misconduct.

Any reference in this Policy to any law or legislation is to the same as such may be amended, modified or replaced from time to time.

5 Queries

If you have any queries on this Policy and/or if you have any issues in relation to passwords, data backups, encryption, data protection and any IT Security or IT Acceptable Usage issue please contact the Services Desk in the first instance and then the IT Manager as may be required.

6 Violation of Policy

If you want to report a suspected security breach of this Policy including a password or access break, or a lost/stolen storage device, please contact the Services Desk in the first instance and then the IT Manager as may be required.

If you have any issues in relation to passwords, data backups, encryption, data protection and any IT security or IT acceptable usage issue please contact the Services Desk in the first instance and then the IT Manager as may be required.

Contravention of this Policy may lead to the removal of privileges relating to CIT Resources and/or CIT Data and may lead to disciplinary action in accordance with the Institute's disciplinary procedures. For more information in this regard please see the "Protocol for Dealing with Suspected Breaches of CIT's Computer Systems Acceptable Usage Policy" in Appendix 1.

7 General

Headings used in this Policy and the documents attached in Appendix 1 are for ease of reference only and shall not affect their construction.

Unless the context otherwise requires, any reference in this Policy to any gender includes the other and to the singular shall include the plural and vice versa.

Words not otherwise defined in this Policy that have a well-known and generally accepted technical or trade meaning in the IT industry in Ireland are used in this Policy in accordance with such recognised meaning.

Unless otherwise defined therein, capitalised terms used in the documents attached in Appendix 1 shall have the same meaning as given to them in this Policy.

This Policy is reviewed periodically as required and CIT reserves the right to amend it at any time as it sees fit.

This Policy supersedes and replaces any previous policy relating to its subject matter. In the event of any inconsistency between the provisions of this Policy and the provisions of the documents attached in Appendix 1 to this Policy, the provisions of the Policy shall take priority.

8 Appendix 1: Related Operational Procedures


CUP Guidance on Anti-Virus.doc


CUP Guidance on Passwords.doc


Content Review Procedures.doc