



Institute of Education University of London

Computer Security Policy

Contents

1	Information Security Policy Statement.....	3
1.1	Introduction	3
1.2	Regulatory compliance environment.....	4
1.3	Usage monitoring	5
1.4	Security breaches	5
1.5	Policy awareness and disciplinary procedures.....	6
1.6	Supporting Policies, Codes of Practice, Procedures and Guidelines	6
1.7	Information security policy status	6
2	Policy 1: Data Protection Act 1998 Compliance	7
3	Policy 2: Electronic Messaging.....	8
3.1	Introduction	8
3.2	Accessing Institute Email and other Electronic Communications.....	8
3.3	Email Security	8
3.4	Appropriate Use of Institute Email Systems	9
3.5	Unacceptable Use of Email Systems	9
3.6	Privacy	9
4	Policy 3: Conditions of Use of the Institute of Educations Information Systems	10
4.1	Policy on Access and Use of Information Systems	10
4.2	Conditions of use of Information Systems provided by the Institute of Education 10	
4.3	Scope.....	12
4.4	Permission to use IS systems	12
4.5	Usage	13
4.6	Compliance	14
4.7	Commercial Usage	16

4.8 Confidentiality	16
4.9 Breach of the Regulations.....	17
4.10 Disclaimer	17
5 Guidelines for the use of Electronic Information Services provided by the Institute of Education.....	18
5.1 General Principles.....	18
5.2 Physical Security.....	19
5.3 Computer System Access.....	19
5.4 Use of Shared Network Resources and Home Drives (N:)	20
5.5 Virus Prevention and Detection.....	22
5.6 Laptops, Wireless Networks and web based Virtual Private Network.....	22
5.7 Use of Controls/Monitoring Tools.....	25
5.8 Internet and other Public Services	26
5.9 Use of Electronic Messaging Systems.....	27
5.10 Legal and Regulatory Compliance	28
5.11 Reporting Security Incidents and Local Contacts.....	30
5.12 Backup and Restoration of Data	30
5.13 Software Acquisition.....	31
5.14 Prohibited Software.....	32

1 Information Security Policy Statement

1.1 Introduction

- 1.1.1 Information is vital to the success of the Institute of Education, most importantly on an academic level and on a business level; how we acquire it, our ability to use it and the way we share it. Behind all of these activities is the critical need for effective data security to ensure the confidentiality, integrity and availability of our data and information systems. Effective security is achieved by working with appropriate conduct, in compliance with legislation, Institute policies and by adhering to approved codes of practice.
- 1.1.2 The Director of Administration and Institute Secretary is responsible for the approval of all of Information Services policies and ensuring that they are discharged to the relevant heads of department/faculties.
- 1.1.3 This information systems security policy is the Institute of Education's approach to information security as well as being a method to establish a set of tools to outline the responsibilities necessary to safeguard the security of the Institute's information systems with supporting policies, codes of practice, procedures and guidelines.

Scope

- 1.1.4 The policy applies to all staff and students of the Institute as well as all other authorised users. The policy relates to the use of all Institute-owned information system assets, to all privately owned systems when connected directly or indirectly to the Institute's network and to all Institute-owned and or licensed software/data.

Objectives

- 1.1.5 The primary objectives of this policy are to:
- Ensure the protection of all Institute information systems (including but not limited to; all computers, networking equipment, software and data) and to mitigate the risks associated with the theft, loss, misuse, damage or abuse of these systems.
 - Make certain that users are aware of and comply with all current and relevant UK and EU legislation.
 - Provide a safe and secure information systems working environment for staff, students and any other authorised users.

- Make certain that all of the Institute's authorised users understand and comply with this policy and any other associated policies and adhere to and work inline with the relevant codes of practice.
- Protect the Institute from liability or damage through the misuse of its information systems facilities.
- Ensure that all users understand their own responsibilities for protecting the confidentiality and integrity of the data that they handle.

1.2 *Regulatory compliance environment*

1.2.1 As an organisation the Institute of Education has a responsibility to abide by and adhere to all current UK and EU legislation. If required further information on legislation relating to the Institute's policies can be found in the supporting guidelines documents. Of particular importance are the Computer Misuse Act 1990 and the Data Protection Act 1988. These policies make provision for the Data Protection Act's requirement for a formal statement of the Institute's security arrangement for personal data. Listed below is some of the relevant legislation;

- The Computer Misuse Act 1990
- Data Protection Act 1988
- Regulation of Investigatory Powers Act 2000
- Copyright, Designs and Patents Act 1988
- Defamation Act 1996
- Obscene Publications Act
- Protection of Children Act 1978
- Criminal Justice Act 1988

1.2.2 Further information and summaries of the legislation relevant to the Institute's security policy can be found in the supporting guidelines documents. If required the full texts of the relevant legislation can be found in the Institute's Information Services department.

1.3 Usage monitoring

- 1.3.1 Authorised members of the Systems Support Group will from time to time monitor the information systems under their control. The monitoring of the Institute's information systems may include the monitoring of electronic messaging (email) and communications and access to other external resources such as the internet and World Wide Web.
- 1.3.2 The main reasons for the Institute of Education employing the use of control and monitoring tools are outlined in the list below;
- To track and control the flow of network traffic and to investigate or detect unauthorised use.
 - To facilitate and better improve capacity planning.
 - To maintain good availability of network bandwidth.
 - To protect the security of the Institute of Education's information resources.
 - To avoid or mitigate legal liabilities and comply with legal obligations.
 - To prevent and detect crime.
- 1.3.3 Within the terms of the Regulation of Investigatory Act (RIPA) 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 provisions for this monitoring have been made. The above mentioned Regulations establish formal notice that communications may be intercepted for reasons allowed within these Acts.

1.4 Security breaches

- 1.4.1 The Institute's Information Services department routinely monitors network activity, alerts and notifications from JANET CERT (Computer Emergency Response Team) and other security advisories to ensure that actions taken and or recommendations made are in line with maintaining the security of the Institute's information systems.
- 1.4.2 All staff, students and other authorised users suspecting that there has been or is likely to be a breach of security have a duty to immediately inform their head of Faculty/Department or the IS Helpdesk who will advise the Institute on the action to be taken.
- 1.4.3 In the event of a suspected or actual security breach Information Services may, after consultation with the relevant head of department/faculty, authorise the action to disable/remove any usernames, data from the network or anything else deemed reasonable to secure the Institute's information systems.

- 1.4.4 Any security breach of the Institute's information systems could lead to the possible loss of security of any personal information stored on these information systems. This is in itself an infringement of the Data Protection Act 1998 and may result in criminal or civil action against the Institute. Therefore it is crucial that all users of the Institute's information systems adhere to this policy as well as the Institute's Data Protection Policy.

1.5 Policy awareness and disciplinary procedures

- 1.5.1 A copy of this policy will be distributed to all new members of staff by the Human Resources Department and to all new students by the Registry. All current staff, students and other authorised users will be informed of the existence of this policy and the availability of supporting policies, codes of practice and guidelines. The failure of staff, students and other authorised users to comply with this policy may lead to the instigation of the relevant disciplinary procedures up to and including dismissal. In certain circumstances, legal action may be taken. In the case of a contractor failing to comply with this policy the result may be that the contract with the 3rd party is cancelled and where appropriate reported to the relevant authorities, including the police.

1.6 Supporting Policies, Codes of Practice, Procedures and Guidelines

- 1.6.1 Supporting policies have been developed to strengthen and reinforce this policy statement. These, along with associated codes of practice, procedures and guidelines are published together and are available for viewing on the Institute's website. All staff, students and any third parties authorised to access the Institute's network are required to familiarise themselves with these supporting documents and to adhere to them in the working environment.

Supporting policies

Policy 1: Data Protection Act 1998 Compliance

Policy 2: Electronic Messaging

Policy 3: Conditions of Use of the Information Systems (Draft 1)

1.7 Information security policy status

- 1.7.1 Whilst these policies do not form part of a formal contract of employment with the Institute, it is a condition of employment that employees abide by the policies made by the Institute from time to time. These policies also form an integral part of the student regulations.

2 Policy 1: Data Protection Act 1998 Compliance

This is currently under preparation by the Institute of Education's Assistant Secretary.

3 Policy 2: Electronic Messaging

3.1 Introduction

3.1.1 The Institute of Education provides a number of electronic messaging systems as an active means for communication. This ensures that there is an efficient method in place to facilitate a large portion of the Institute's business. This policy sets out the proper use of email for Institute related purposes. All users of the Institute email systems can find further information in the accompanying guideline documents.

3.2 Accessing Institute Email and other Electronic Communications

3.2.1 Institute email access is given to all staff; students and approved third parties who agree to adhere to and abide by the Institute's policies, codes of practice and guidelines.

3.2.2 The Institute email services are provided to staff, students and approved third parties to conduct official Institute-related business. Personal email is not official Institute business, although incidental and occasional personal use of email is acceptable so long as it does not disrupt or distract the individual from the conduct of Institute business or cause the restriction of use of these systems to other legitimate users.

3.3 Email Security

3.3.1 Unless email is encrypted during transit all users should assume that privacy cannot be guaranteed. It is akin to sending a postcard through the post; therefore care should be taken when addressing email to recipients.

3.3.2 The Institute has put into place spam filters and anti-virus filters at the email gateways. These filters are there to protect the Institute of Educations information systems resources from viruses and unsolicited email. Whilst the Institute is constantly updating these filters it cannot guarantee that it will provide 100% protection against all viruses and spam. If any users feel that they are receiving excessive amounts of unsolicited email or are being caused distress by the receipt of offensive email they may contact the IS helpdesk for further guidance.

3.3.3 Through the use of encryption the Institute provides a secure web based access method for all users with an Institute email account. This can be accessed through a supported web browser from any location with internet access. Further information on this is provided in the accompanying Guideline documents.

3.4 *Appropriate Use of Institute Email Systems*

- 3.4.1 The use of Institute provided email is subject to all relevant laws, policies, codes of practice and guidelines. All users must comply with the Institute Policy on the Conditions of use of Information Systems Facilities at the Institute.

3.5 *Unacceptable Use of Email Systems*

- 3.5.1 If a complaint is raised or it is suspected that an Institute provided email account is being used improperly then the Head of Information Services may authorise an initial investigation. If the complaint or the suspected misuse appears to have reasonable basis then further investigatory measures may be initiated in line with other Institute policy and regulations.
- 3.5.2 The failure to adhere to and comply with this email policy could result in the email facility for individual users being withdrawn or in more serious cases disciplinary procedures being invoked and possible referral to the relevant authorities such as the police.

3.6 *Privacy*

- 3.6.1 Under the terms of this policy no person shall monitor another user's email account unless authorisation has been granted to do so. The monitoring and or inspection of email accounts may only occur in accordance with Section 3 of the Information Security Policy and under the heading of Use of Controls/Monitoring Tools set out in the Guidelines for the use of Electronic Information Services provided by the Institute of Education.
- 3.6.2 The Institute in accordance with its legal and audit obligations and for legitimate operational purposes reserves the right to access and disclose the contents of a users email message or messages. The Institute also reserves the right to demand where necessary the disclosure of decryption keys so that it may fulfil its right of access to a users email messages in such circumstances. The Institute also reserves the right to monitor a users email account where necessary as set out in Section 3 of the Information Security Policy and under the heading of Use of Controls/Monitoring Tools set out in the Guidelines for the use of Electronic Information Services provided by the Institute of Education in line with the Regulation of Investigatory Powers Act (RIPA) 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.

4 Policy 3: Conditions of Use of the Institute of Educations Information Systems

Regulations for the Use of Information Systems (IS) Facilities

4.1 Policy on Access and Use of Information Systems

- 4.1.1 This document sets out the policies and codes of practice for the use of the Institute of Education's IS Facilities. These apply to all members of staff, students and all other users authorised to use the IS facilities.
- 4.1.2 The following Summary is provided so that all users of the IS facilities provided by the Institute of Education can more easily understand their obligations and responsibilities when doing so.

4.2 Conditions of use of Information Systems provided by the Institute of Education

- 4.2.1 Before any use may be made of any of the computing or networking facilities provided by the Institute of Education you must first register as a user. If you are a student or a member of staff of the Institute of Education and your status as such is properly recorded in the relevant administrative databases you will be registered as a computer user by way of an automatic process. As part of the registration process you will be required to accept these policies for the Use of IS Facilities.
- 4.2.2 As part of the registration process you will be given a unique user name and a password. This user name is your personal identification and along with your password serves to authenticate you to the system and to grant access to the information resources you have been authorised to use. You must keep your password secure and secret at all times. You should not allow any other individual(s) to access the computer facilities by way of your user name nor should you use or attempt to use the facilities through someone else's user name. You should not do anything that attempts to find out another user's user name/password combination. Any attempt to gain access to information or facilities owned by another user is prohibited. All of these activities could technically be construed as offences under the Computer Misuse Act and therefore illegal.
- 4.2.3 In general, your use of the computing and networking resources that you have been authorized to use should be to support your area of work, study or research. It must not interfere with or cause difficulties for other users of the IS facilities.
- 4.2.4 As a user you will have access to email facilities. These are primarily provided to improve communications amongst staff and students for matters relating to their

roles within the Institute of Education. It has been agreed that the Institute of Education will permit the limited use of the email systems provided for personal and social purposes but such use should not become excessive nor should it interfere with your day to day duties. Sending harassing, insulting, abusive, defamatory or otherwise offensive messages or material by email is not permitted and will not be tolerated.

- 4.2.5 When using email, or any of the other computer messaging facilities, the system will normally include some sort of electronic information that uniquely identifies the sender. Any attempt to change this information so as to disguise or hide your identity or to pretend to be, or impersonate someone else is not acceptable, and may in fact be illegal.
- 4.2.6 As a registered user of the Institute of Education's IS facilities you will also have access to large quantities of information that is available through the network, particularly via the Internet and the World Wide Web. These facilities are provided primarily to enable access to information relevant to your work, study and research within the Institute of Education. Limited use for leisure or simple curiosity purposes is permitted, however, this should not be excessive nor should it involve access to material of a nature which might bring discredit to you and/or the Institute of Education, for example the viewing of pornographic, criminal, defamatory, discriminatory or offensive material is forbidden. If you need to access information which might be questionable as part of your particular work, study or research you should seek formal authorisation in advance from your head of department and the Head of IS/Head of Technical and User Support should be notified.
- 4.2.7 There are many ways that you, as a user of the IS facilities, will be able to make information available to other users of the Institute of Education's network and/or externally to users of the World Wide Web and Internet. If you are publishing electronic information then you must adhere to the Electronic Publishing Policy and Guidelines, and nothing should be published in a way which could be considered discreditable to the Institute of Education. Again, if publication of questionable material is essential as part of your academic work, this should be cleared in advance with your head of department and the Head of IS/Head of Technical and User Support.
- 4.2.8 The Institute of Education operates the usage of and access to its IS facilities on the basis of trust. However, if there are reasonable grounds for suspecting that an individual is engaging in activities which are in breach of the Institute of Education's policies and regulations or of the various guidelines provided, the Institute of Education reserves the right to investigate fully. This includes but is not limited to the direct monitoring of the use made by the suspected user. In the event that the serious misuse is suspected the Institute of Education will take appropriate disciplinary action and if criminal behaviour is detected it will have no hesitation in reporting the matter to the Police or relevant law enforcement agency.
- 4.2.9 The Institute of Education exercises its right to monitor the use of facilities to ensure that usage is within the terms of the policies and guidelines set out by the Institute of Education. Such monitoring can, when necessary, include monitoring

and reading electronic communications and access to external resources (including web sites).

4.2.10 As a feature of your use of the computing facilities you will gain access to a large amount of software and other computer based information. In nearly all circumstances this material is subject to copyright restrictions. Under no condition are copies of this material to be made without the prior approval of the copyright owner. Software in particular may not be copied for use on other machines nor may it be passed on to other people, even other users within the Institute of Education, unless explicit permission to do so has been granted by the copyright owner or the relevant software license has been obtained.

4.3 Scope

4.3.1 These Regulations apply to the use of all computer, electronic information and communication facilities at or operated wholly or partly by the Institute of Education including;

- All local (on-site) computing facilities, server systems, work stations, personal computers, personal systems connected via the data networks (wirelessly or through the use of VPN technology or both) or other electronic information and communication systems whether provided by the Institute of Education or otherwise and which are intended wholly or partly for use by employees of, contractors, researchers or students of the Institute of Education or wholly or partly for use for other Institute or Institute related academic purposes.

4.4 Permission to use IS systems

4.4.1 Within the Institute of Education's IS facilities, all IS systems will be under the control of a System Owner.

4.4.2 This System Owner has the control to evaluate and allocate users of that System, to refuse any request or application to use that system and to implement the 'Conditions of Use' of that System by a user as deemed suitable.

4.4.3 The conditions of use will include the System Owner issuing, and recording in the relevant database, a unique User Name for a user and they will also enforce the user to adopt a personal password, in line with the password guidelines, for the purposes of identifying and authenticating the user when gaining access to an authorised System or Systems.

4.4.4 The System Owner/s may at any time add to, delete or amend, as they see fit, any 'Conditions of Use' applicable to any user.

4.4.5 The permissions granted to a user to use a system or systems are limited to the user to whom permissions have been granted, in particular:

- Any permission given to a user may not be extended or transferred to any other person or persons unless authorised by the system owner/s;
- The user may not, under any circumstances, allow any other person (whether a user or otherwise) to access an Institute of Education system or systems by way of their personal User Name and personal password. All users are required to keep and maintain their username/s and password/s secret at all times;
- All users must not use or access a system beyond that limit for which permission has been granted to those users;
- A user must not access a system and leave it in such a state that it becomes available to another person (for example, locking workstations, exiting applications or logging off the system).

4.5 Usage

4.5.1 The user agrees and accepts that:

- Use of the Institute of Education's IS facilities, such as the network, wireless network, telephone network, workstations, printers, photocopiers and all the facilities associated with these e.g., software, data, email, world wide web (www), online learning and databases but not excluding any other part of the Institute of Education's computing systems, must be for the expressed purpose of research, teaching, learning, coursework, associated administration or other appropriate authorised use. No 'private' work is permitted without prior authorisation from department heads and committees and in accordance with relevant policies.
- All data/programs created/owned/stored by the user on or connected to the Institute of Education's IS facilities may in the instance of suspected wrong doing, be subjected to inspection by Institute designated Officers. In cases where the data/programs are in an encrypted state the user shall be required to provide the decryption key in a timely manner to facilitate decryption of the data/programs. If the material is found to be in contravention of any of the Institute of Education's policies including misuse and/or of an illegal nature then disciplinary procedure will be invoked and if necessary the relevant legal authorities notified.

4.6 Compliance

4.6.1 All users must comply with all relevant policies, codes of practice, guidelines, staff and student regulations in force and applicable to IS facilities provided by the Institute of Education and third parties(such as JANET). Specifically but not exclusively, the user must:

- Use the System in compliance with the current statutes and legislation of England and its territories. English legislation that has been shown to be relevant to the use of Information and Communication Technology includes the following:
 - Anti-terrorism, Crime and Security Act, 2001
 - Computer Misuse Act, 1990
 - Copyright (Computer Programs) Regulations 1992
 - Copyright, Designs & Patents Act 1988
 - Criminal Justice and Public Order Act 1994
 - Data protection Act, 1998 and the EU Directive on Data Protection (incorporating the Safe Harbor agreement)
 - Freedom of Information Act
 - Human Rights Act 1998
 - Protection from Harassment Act 1997
 - Obscene Publications Acts
 - Regulation of Investigatory Powers Act, 2000
 - Telecommunications Act 1984
 - The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

4.6.2 Adhere to the terms and conditions of all license agreements relating to the Institute of Education's IS facilities which they use including software, equipment, services, documentation and other goods.

4.6.3 Have a primary responsibility for the security and back-up of their work and data, the central back-up of the Institute's core systems is for the sole purpose of disaster recovery and business continuity. It is not for restoring data that users have deleted accidentally.

4.6.4 Ensure that when using any of the material and software made available by the Institute of Education that the copyright of this material is respected and remains intact, and not to use, copy, store or distribute copyright material unless explicit permission to do so has been granted by the copyright owner and/or the relevant software license has been obtained or under the terms of the license held by the Institute of Education.

4.6.5 If holding or processing data on computers about living individuals you must register that data and its uses, in line with the Institute of Education's Data Protection Act Policy, procedures and guidelines and handle it in strict accordance with the 8 Principles, as set out by the Data Protection Act 1998. Student users wishing to construct or maintain computer files of personal data for use in connection with their academic studies/research must seek the expressed

authorisation of an appropriate member of staff, normally their supervisor or head of department and the Institute of Education's Data Protection Officer.

4.6.6 All users of the Institute of Education's IS facilities shall not, knowingly or negligently:

- Make use of, or access a System for any illegal or unauthorised purpose;
- Store or make accessible (publicly or otherwise) any data, text, image or program which is unlawful or, whether lawful or not, could bring the Institute of Education into disrepute or damage its reputation or is not in line with the principles, goals, aims or objectives of the Institute;
- Attempt to reverse-engineer any part of a System (including software) without the written permission of the copyright owner;
- Create, store, process or transmit any defamatory material or material which is designed or likely to cause harassment or needless annoyance, inconvenience or anxiety to another be they a user of the Institute of Education's IS facilities or not;
- Disclose to others her/his login name/password combination(s) or access or attempt to access computers or computing services at the Institute of Education or elsewhere for which permission has not been granted or facilitate such unauthorised access by others;
- Use or produce materials or resources to facilitate unauthorised modification, access, changes, malfunction or access to any Institute or external IS facilities;
- Display, store or transmit images or text likely to cause offence in an academic community, e.g. material of a sexual, pornographic, sexist, racist libellous, threatening or defamatory nature or likely to bring the Institute into disrepute, without notification to their supervisor (for students) or Head of Department (for staff) setting out the reasons why the material is required to support legitimate research or scholarship;
- Forge email signatures and/or headers, initiate and/or forward 'chain' or 'junk' or 'harassing' mail;
- Attempt to install unauthorised software on any system without first obtaining permission from the system owner;
- Attempt to uninstall or disable any software or service on any IS system without the expressed authorisation of the system owner;
- Play unauthorised games.

4.7 Commercial Usage

- 4.7.1 Before any work is to involve commercial usage of any of the Institute of Education's IS facilities (no matter how trivial), the approval of the relevant committee and system owner must be obtained before any use is made of the IS facilities for such work. Whether or not the individual(s) concerned are authorised to use these facilities for educational purposes, further authorisation is required before any form of commercial usage can commence, and an appropriate rate of charges must be agreed by the appropriate committee/Head of IS/Head of Technical and User Support and be in line with Institute policies on external private work.
- 4.7.2 Where any short courses or contracts commence and any of the Institute of Education's IS facilities are to be used in connection with research grants, involving specific provision for computing costs, this fact must be communicated to the Head of IS/ Head of Technical and User Support and a rate of charges must be agreed before such utilisation may commence.
- 4.7.3 Commercial usage of software supplied under educational use only agreements is permitted only if explicit written approval and relevant licenses have been obtained from the supplier of the software.

4.8 Confidentiality

- 4.8.1 The Institute of Education will employ best effort, through its system owners and internal processes and procedures, to protect information stored on or by means of any Institute owned IS systems. However the Institute of Education will not be responsible nor will it be held accountable for upholding any special restriction or condition on the handling or usage of any information unless it has been informed of the existence of such restriction or condition and has agreed to enforce it.
- 4.8.2 All users of the Institute of Education's IS facilities processing personal data must ensure that they comply with the Institute of Education's Data Protection Act Policy, procedures and guidelines. The Institute of Education maintains a general registration / notification under the Data Protection Act that should cover most of the data that would be used solely for academic purposes. If you are in any doubt about your obligations under the Data Protection Act then you must consult the Institute's Data Protection Officer.
- 4.8.3 A user's name, address, photograph, status, email name, login name, alias and/or other related information may be stored in a computerised format for use for administrative and other operational purposes (e.g., monitoring system usage).

4.9 Breach of the Regulations

- 4.9.1 The Head of Information Services or designated officers have the right to withdraw or delete any users account (either temporarily or permanently) and/or the permissions of any user to use any IS facility in circumstances where those mentioned above have reasonable grounds to believe that a user or users have breached these policies.
- 4.9.2 A breach of these Regulations may also constitute a criminal or civil offence, for example under the Computer Misuse Act 1990, the Protection from Harassment Act 1997, the Anti-terrorism, Crime and Security Act, 2001. Non-compliance with these Regulations may also constitute a breach of the Copyright, Designs & Patents Act 1988. In the event that the Head of IS/ Head of Technical and User Support or designated officers suspects that any user may have committed an offence, the police or other appropriate enforcement authority may be contacted to investigate whether an offence has been committed.
- 4.9.3 In addition to the possible sanctions in these policies, suspected non-compliance with these policies may also be investigated in accordance with the Institute of Education's internal disciplinary procedures as set out by Human Resources and the Student Body. A significant breach of these policies may be regarded as gross or serious misconduct and could result in dismissal or removal from study.
- 4.9.4 Any user or users who are in breach of these policies, (whether directly or indirectly e.g. by giving unauthorised permission to someone who is not a registered user or another user to use a System) will indemnify and hold harmless the Institute of Education against all costs incurred by and losses caused to the Institute by reason of such breach, including (but not limited to) repair costs, any claim for damages, legal costs, fines or other financial penalties.

4.10 Disclaimer

- 4.10.1 The Institute of Education takes responsibility for providing and operating systems with due care and skill, but it in no way accepts liability for any loss or damage any user may suffer from any failure or malfunction of a system or systems.
- 4.10.2 Whilst the Institute of Education takes appropriate security measure, in line with industry best practice against unauthorised access to, alteration, disclosure, destruction, theft, deletion or accidental loss of personal and other data it cannot and does not give any warranties or guarantees to the users of IS facilities about the security, confidentiality or integrity of data, personal or otherwise.

5 Guidelines for the use of Electronic Information Services provided by the Institute of Education

5.1 General Principles

We recognise and have taken into consideration the fact that the Institute of Education is a specialist University that is aimed at the research and improvement of education, and prides itself on this fact. We therefore encourage staff and students alike to make full use of the information systems in place, where such use is suitable for the purpose of study/academia/business and supports the goals and objectives of the Institute without abusing them in accordance with this document. The Institute of Education feels that these guidelines will help you to do so in line with all Institute approved policies whilst not restricting your academic freedom, therefore if you have any requirements relating directly to your research, study or work they should be brought forward to Information Services and best efforts will be made to ensure access to specifics. Access will either be allowed or denied based on a decision whether or not the requirement poses a threat to the security of our information systems.

The Institute of Education's network and computing systems not only cover in house systems such as databases/Content Management Systems/Management Information Systems, wireless networks, voice over IP telephone systems, web servers, data servers but also email, the Internet and remote access through virtual private network technology. The systems are to be used in a manner that is consistent with the way you would carry out your normal day to day studies, research or work duties and inline with Institute values.

The Institute of Education has software and hardware technology in place that can monitor and record all network usage. This includes internet usage and file transfers to and from our networks. The Institute of Education reserves the right to do this at any time for the purposes set out under section 3 of the Information Security Policy, this is further covered in these guidelines under the title of Use of Controls/Monitoring Tools and you consent to such monitoring. No user should have any expectation of privacy as against the Institute of Education in regards to their Internet usage. The Institute of Education reserves the right to inspect any and all files stored on any Institute computing resource to ensure compliance with this policy this may in some cases include electronic messaging.

Whilst the Institute has in place systems for screening email for virus and spam it should be noted that screening of email content and filtering of web sites visited does not take place. The Institute's Information Strategy Committee made the decision that this type of screening would be incompatible with the Institute's academic remit, mission and values.

5.2 Physical Security

The security of the Institute of Education's computing resources and information begins with physical security measures to prevent unauthorised access and theft. The following applies:

- For staff, query the presence of any strangers in your work area.
- Lockup laptop computers, PDAs, disks, removable media containing sensitive information and sensitive documents when you are away from your office or workstation.
- Do not remove any computer equipment or media from the Institute unless authorised to do so.
- Ensure that only devices that are approved by IT management are connected to the Universities network or communication/computing equipment.

5.3 Computer System Access

The Institute of Education computing resources, data, information and information processes must be protected from unauthorised use, external intrusion and accidental or malicious damage.

5.3.1 Protecting Active Sessions

An unattended computer may provide an opportunity for unauthorised access to the Institute of Education computing resources and information.

- Close down active sessions and log out of, or lock your workstation using the Ctrl+Alt+Delete buttons if you intend to leave it unattended.
- Log out of your workstation every day when going home or leaving the Institute. Do not however, under any circumstances, turn your computer off as essential network maintenance is carried out during the night (unless instructed to do so by a member of Information Services). It is critical that all machines be left on, even if you are leaving the Institute for a long period of time. If you wish to conserve energy turn only the monitor off.
- Do not store sensitive information on your local drive unless it is protected with access controls or encryption software.

5.3.2 Passwords

A username combined with your password is your unique key for accessing the Institute of Education's computing resources and information systems. It is therefore important to choose a strong password and guard it carefully. The password guideline applies to all staff and students without exception.

- The minimum length of your password is 8 characters. Information Services will enforce users to use a combination of uppercase, lowercase and numeric characters. A history control of your password will also be enforced so that you can not reuse any of your last 3 passwords. Your account will be locked after 6 failed logon attempts. If this happens, only an administrator will reset your password for you and you must present yourself to the computer helpdesk on level three in the library with a form of staff or student id for this to happen.
- Do not reveal your password to anyone, including family or friends.
- Do not store your password with your user name or workstation at any time.
- Change your password immediately if you think it has been compromised.
- Do not reuse passwords.

5.4 Use of Shared Network Resources and Home Drives (N:)

The Institute of Education provides individual and shared disk space to all staff and students for the purpose of storing and sharing appropriate data relating to your work/study or research. These individual (your home drive (N:)) and shared network storage areas (O: drive for staff and students and the Q: drive for staff only) are not infinite resources and everybody has a responsibility to ensure that these network storage areas are managed effectively. This can only be done by regularly reviewing their content and removing unnecessary and/or out of date material. Information Services will regularly use monitoring tools to ensure compliance with this policy (later referred to under use of controls and monitoring tools).

5.4.1 O: drive (for staff and students)

The O: drive has been created for the sole purpose of providing an area where staff can place the relevant teaching material needed for them to better deliver courses being taught to students. Please note that students only have read access on the O: drive and only staff authorised by Information Services are allowed to write to the O: drive to share information with students. Please abide by the information below:

- It is NOT an alternative area for staff to store data that is not directly related to the courses being taught to students, even if it is temporary.

- The staff that have been assigned the responsibility for maintaining files and folders on the O: drive are encouraged to regularly review the material stored here and remove any of the unnecessary and/or out of date material.

5.4.2 Q: drive (for STAFF only)

The Q: drive has been created to provide faculties and departments with the ability to make important and/or sensitive data available to other relevant staff within these areas. This means that it is a safe area to store and share data that only authorised people may view in your faculty or department.

Please abide by the information below:

- Staff that have been assigned the responsibility for maintaining these files and folders for their department are encouraged to regularly review the material stored here and remove files and/or folders that are no longer required or out of date.
- The Q: drive is NOT an alternative area for staff to store their own data, only data that needs to be shared with others in the faculty or department may be stored here.

5.4.3 Home Drives (your N: drive for staff and students)

All staff and students with an Institute of Education computer user account are provided with a storage area; this is referred to as your N:\ drive and is automatically connected when you log in. All users N:\ drives are backed up regularly to ensure that in the event of data corruption or disaster the IT department has the capability to recover the information (further referred to in the Backup and Recovery section). Therefore the N:\ drive is an area that should only be used to store critical data in relation to your work/study or research. All users must abide by the following information.

- It is NOT an area for staff or students to store personal data such as programs, pictures, movies or music that does not relate directly to your study/work or research.
- All users (unless otherwise arranged with Information Services) will be subjected to a disk quota management system, similar to that enforced on your email mail box size. This means you, the user, will be allocated a set amount of network storage disk space that will not exceed 3 Gigabytes for staff and 500 Megabytes for students. Information Services will use this quota management software to monitor the use of this storage space to ensure compliance with this policy.
- Staff and students have an obligation to regularly review the data stored on their N:\ drive and delete or remove out of date files and folders. This is to ensure that your user area remains free from old data taking up valuable space.

5.5 Virus Prevention and Detection

Computer viruses can destroy data and cause machine malfunctions. Software, electronic documents and floppy disks can all carry viruses. The Institute of Education has gone to great lengths to ensure all machines owned by the Institute and on the Universities network are up to date with the latest version of the Anti Virus product that we use.

The Institute of Education takes a layered approach to virus threats by using two different types of Anti Virus software. The most commonly used of these is the Anti Virus which is run on all desktop computers at the Institute. New software updates and virus signatures are checked for and downloaded if necessary from a central data bank to a server at the Institute. This server will then remotely update all of the desktop machines in the Institute, this can happen up to four times daily. We therefore remind all computer users to ensure that desktop computers are to remain switched on at all times.

The other Anti Virus solution used is on our servers and scans incoming email and all files on our data servers. These two Anti Virus solutions help the Institute to mitigate the risks viruses pose and to cover all areas where a virus might try to get onto our network through deliberate or accidental means.

We ask all students and members of staff to follow this guide to minimise the impact of viruses on the Institute of Educations information systems.

- Ensure that installed virus protection software is not deliberately disabled or prevented from running.
- Scan all floppy disks, CD ROMs or other media originating from external sources. This includes media last used on a home computer, or any other external network.
- Scan all software and electronic documents acquired from third parties and external networks, such as the Internet or email.
- Scan all floppy disks before you distribute them to others.
- Report the suspicion of any virus to IT Support staff immediately.

5.6 Laptops, Wireless Networks and web based Virtual Private Network

The purpose of this section is to define standards for connecting to the Institute of Educations network from any host other than the workstations within the Universities buildings provided for staff and students. These standards are designed to minimise the potential exposure to the Institute of Education (with particular reference to viruses, malicious code and accidental or intentional damage) from unauthorised use of the Institute of Educations information technology resources. The Institute of Education has

made available a campus wide wireless network through which staff and students can access internal resources through the Institute of Education's web based virtual private network which is referred to as the IOE portal. The IOE Portal is also available from any computer in any location that has a web browser outside the Institute's internal network. It is not available from any internal Institute network except the wireless network.

5.6.1 Laptops: Staff

The following procedures must be followed before any staff laptop can connect to the Institute of Educations internal network:

- All Institute purchased laptops must be brought to the helpdesk where they will be setup for use on the internal network. This procedure will include the setting up of the operating system and installation of software approved by the Institute of Education. Most importantly the laptop will be configured to automatically download and install Microsoft security updates. It will also have Symantec Anti Virus installed and configured to automatically check and download virus updates if necessary from the Symantec website.

5.6.2 Wireless Network: Staff

All the information for staff wanting to utilise the wireless network can be found by clicking on the following web link.

http://ioewebserver.ioe.ac.uk/ioe/cms/get.asp?cid=8928&8928_0=10839

5.6.3 IOE Portal (SSL VPN): Staff

All the information for staff wanting to utilise the IOE Portal can be found by clicking on the following web link.

http://ioewebserver.ioe.ac.uk/ioe/cms/get.asp?cid=11549&11549_0=10838

5.6.4 Laptops: Students

Under no circumstances are student laptops to connect directly to the Institute of Educations internal network. The Institute's IT department has made provisions for students to gain access to the internet and other resources through the use of a wireless network and the IOE Portal. The Institute's wireless network is available throughout all of its buildings. In order to make use of wireless network you must be a registered user here at the Institute. All staff and students are automatically given access to use the wireless network and the IOE Portal.

5.6.5 Wireless Network: Students

All the information for students wanting to utilise the wireless network can be found by clicking on the following web link.

http://ioewebserver.ioe.ac.uk/ioe/cms/get.asp?cid=8929&8929_0=10836

5.6.6 IoE Portal: Students

All the information for students wanting to utilise the IOE Portal (SSL VPN) can be found by clicking on the following web link.

http://ioewebserver.ioe.ac.uk/ioe/cms/get.asp?cid=11549&11549_0=10838

5.6.7 Laptops: Visitors

Visitors wishing to make use of the wireless network need to report to the helpdesk where a temporary username and password will be issued and internet only access will be provided. This facility is only available to visitors on official Institute of Education business and conference attendees. It is not available to the general public.

5.6.8 Wireless Network: Visitors

All the information for visitors wanting to utilise the wireless network can be found by clicking on the following web link.

http://ioewebserver.ioe.ac.uk/ioe/cms/get.asp?cid=8820&8820_0=10840

5.6.9 Remote Access

This applies to all Institute of Education staff, students and 3rd party organisations with an Institute of Education owned or personally owned computer that is used to connect to the Institute of Education's internal network. This refers to remote access connections used to do work on behalf of the Institute of Education and includes reading and sending mail as well as using internal network resources. Remote access implementations include but are not restricted to Virtual Private Networking, Secure Shell, Telnet and ISDN. Please abide by the following information.

- It is the responsibility of the Institute staff, 3rd party contractors and vendors with remote access privileges to the Institute of Education's internal network to ensure that their remote access connection is given the same consideration as the users' onsite connection to the Institute of Education's network.
- It is also the responsibility of those with remote access privileges to ensure that the computer they are connecting from has up to date Anti Virus software installed as well as all critical updates relating to your computer's operating system applied.

- 3rd party connections must comply with requirements as stated in the 3rd party agreement section.
- Institute of Education staff, 3rd party contractors and vendors with remote access privileges must ensure that their Institute of Education owned or personally owned computer which is connected to the universities internal network is not connected to any other network at the same time.

5.7 Use of Controls/Monitoring Tools

The Institute of Education routinely monitor usage patterns for our computerised systems and data communications. The reasons for monitoring are to optimise online productivity, to protect the security of the Universities information resources and to prevent and detect breaches of this policy. More importantly it allows Information Services to trouble shoot faults should they arise and ensure swift detection and resolution. The use of monitoring tools also provides the Information Services with the ability to better manage existing network and computing resources. They also help when planning future upgrades to benefit end users and other purposes referred to in this policy.

Monitoring tools and controls include but are not restricted to anti virus software, network traffic analysers, quota management software for users N:\ drives, patch management software, firewalls and the spam filter.

Monitoring will be carried out by automated software or hardware management tools and managed by authorised members of Information Services (as representatives of the Institute of Education). These software or hardware tools will monitor and record into log files and or databases all information relating to their implementations, whether that be outbound/inbound network traffic through the firewall or users exceeding their email or N:\ drive quotas.

Depending on the nature of your work, research or study you may be given different access rights to the internet, other outside networks or the different systems the Institute has available. The Institute of Education reserves the absolute right to block access to certain internet websites/services, other outside networks or the different systems the Institute has available if we consider it necessary to ensure compliance with this policy and to protect the Universities information resources and users.

The main reasons for the Institute of Education employing the use of control and monitoring tools are outlined in the list below:

- To track and control the flow of network traffic and to investigate or detect unauthorised use.
- To facilitate and better improve capacity planning.
- To decrease network slowdown and keep availability and productivity up.
- To maintain good availability of network bandwidth.

- To protect the security of the Institute of Education's information resources.
- To avoid or mitigate legal liabilities or comply with any legal obligation.
- To prevent and detect crime.
- To monitor quality of service.
- To help maintain a safe working environment.
- To protect the Institute of Education and to protect you.

5.8 Internet and other Public Services

The internet and other public services, such as AOL (America on Line) lie outside the control of the Institute of Education. Information sent in plain text over the internet and other public networks is the equivalent of sending a postcard through the mail. Conducting research and business in these environments requires special precautions to ensure that information within the Institute of Education remains secure and that the acceptable computer use and information security policies are complied with.

Staff and students are asked to limit the use of external systems to activities that support the Institute of Education's objectives both as a University and as a business. Staff, students and 3rd party organisations are asked to be aware that it is now common practice for Universities, organisations and businesses to track their systems usage. The Institute of Education has security devices in place allowing it to track system usage thus enabling the proper implementation of this policy. These will be further referred to in the "Controls and Monitoring Tools" section.

The WWW is an extensively rich, diverse source of information and all staff, students and researchers are encouraged to use it as an additional tool to gather information that is relevant to your work, study or research. However internet browsing can be time consuming, distracting and addictive. It is easy to waste a lot of time browsing/surfing the internet for information that has little use to your work, study or research.

Please take note of the following guidelines which are of critical importance and non-compliance may result in disciplinary action:

It is not permitted to download or view material:

- Of an abusive, racist, sexist, defamatory or pornographic nature.
- That is in breach of current laws relating to publishing and the internet including slander, harassment and copyright laws. This is not an exhaustive list and further information will be outlined in the "Legal and Regulatory Compliance section.
- Of an over zealous recreational nature.
- That could compromise the information security of the Institute of Education at any site.

5.9 Use of Electronic Messaging Systems

The Institute of Education provides electronic messaging systems for all staff and students. This is to facilitate communication among its employees, students and other external bodies i.e. other Universities, research project groups and business partners. These Institute of Education provided messaging systems are the property of the Institute and are intended for Institute business and other Institute of Education sanctioned use. The Institute has put into place a spam filter at the mail gateway. This filter is there to protect the Institute of Educations information resources from viruses and unsolicited email taking up valuable disk space.

While the Institute of Education does not routinely access or monitor individual mail messages or mail boxes (apart from enforcing mail box quotas) there may be instances such as legal, regulatory, security, business reasons or recovery that require electronic messages to be retrieved by the Institute of Education or legal or regulatory agencies.

The Institute of Education reserves the right to retrieve and access electronic messages whether or not they have been marked as confidential, at any time, without the permission of the employee, student or researcher and without notice. Further, once a message has been "SENT", recipients may intentionally or accidentally forward the message to other individuals. Therefore students, researchers and employees should have no expectation that any electronic message will remain private.

Please abide by the following guidelines when making use of the Institute of Educations electronic messaging systems:

- Do not send information that may breach the Universities policies or government regulations. This includes messages that may harass or offend (including racist, sexist information including defamation or obscenity).
- Do not distribute chain mail.
- Do not send messages from someone else's account except under proper "delegate" arrangements which retain individual accountability.
- Do not "auto forward" mail to a non supported system this includes internet and other public networks.
- Do not forward information known or believed to be confidential without the approval of the sender or information owner. If you are unsure whether the information is confidential, assume that it is.
- Take care before entering into contractual agreements by email.
- Do not create email congestion by sending trivial messages or unnecessarily copying emails.
- Ensure you use the appropriate distribution list. If you don't know who is on it, don't use it.

- Ensure that you notify the sender of any email message which you receive in error.

The electronic messaging systems provided by the Institute of Education should not be used for:

- Personal gain or profit.
- To represent yourself as some one else.
- For solicitation to other employees or students.

OR

- When it interferes with your job, study or research or the jobs, study or research of others here at the Institute.
- When it interferes with the Institute of Educations internet and mail gateways.

As a further note to all staff, students and researchers there are a number of file types that are stripped off email messages by the spam filter at the mail gateway. They include the following but are not restricted to:

- .ada,, adp, .bas, .bat, .chm, .cla, .class, .cmd, .com, cpl, .crt, .email, .eml, .exe, .hlp, .hta, .inf, .ins, .js, .jse, .lnk, .msc, msi, .mst, .ocx, .pcd, .pif, .reg, .scr, .sct, shb, .shs, .url, .vb, .vbe, .vbs, .wsc, .wsf, .wsh and .zip.

5.10 Legal and Regulatory Compliance

Below is a list of some of the relevant legislation the all staff, students and the Institute of Education as an organisation must comply with. It is quite often the case that the legislation and regulatory environment we operate in changes, therefore the information below is regularly reviewed and updated. All staff and students are encouraged to make themselves aware of these requirements. Copies of most of the following will be available online (by following the webpage links) or in hard copy from the library and computing helpdesk.

Malicious Communications Act 1988

http://www.opsi.gov.uk/acts/acts1988/Ukpga_19880027_en_1.htm

Data Protection Act 1998

<http://www.opsi.gov.uk/acts/acts1998/19980029.htm>

Computer Misuse Act 1990

http://www.opsi.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm

Regulation of Investigatory Powers Act 2000

<http://www.opsi.gov.uk/acts/acts2000/20000023.htm>

Freedom of Information Act 2000

<http://www.opsi.gov.uk/acts/acts2000/20000036.htm>

Anti-Terrorism, Crime and Security Act 2001

<http://www.opsi.gov.uk/ACTS/acts2001/20010024.htm>

Communications Act 2003

<http://www.opsi.gov.uk/acts/acts2003/20030021.htm>

Protection of Children Act 1978

<http://www.iwf.org.uk/police/page.22.36.htm>

Copyright (Computer Programs) Regulations 1992

http://www.opsi.gov.uk/si/si1992/Uksi_19923233_en_1.htm

Copyright, Designs & Patents Act 1988

http://www.opsi.gov.uk/acts/acts1988/Ukpga_19880048_en_1.htm

Criminal Justice and Public Order Act 1994

http://www.opsi.gov.uk/acts/acts1994/Ukpga_19940033_en_1.htm

Human Rights Act 1998

<http://www.opsi.gov.uk/ACTS/acts1998/19980042.htm>

Protection from Harassment Act 1997

<http://www.opsi.gov.uk/acts/acts1997/1997040.htm>

Obscene Publications Acts 1959 and 1964

Telecommunications Act 1984

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

5.11 Reporting Security Incidents and Local Contacts

As users of the Institute of Education's computing systems you are required to report all information security incidents to your faculty manager, head of department or Computer Helpdesk. The following is a definition of information security incidents;

- An information security incident is defined as an unsuccessful or successful unauthorised access, modification, use, disclosure or deletion of data, interference or modification of normal technology operation or usage of the IT infrastructure in violation of the security and or acceptable usage policy whether it be intentional or accidental. Some examples of information security incident are listed below, but are not limited to;
 - Loss, theft or damage to computing resources.
 - Unauthorised access to computer systems or equipment.
 - Denial of service attacks, intentional or accidental.*
 - Unauthorised use of another user account.
 - Unauthorised modification of a computer system or software.
 - Installation of unauthorised software.
 - Introduction of viruses or malicious software, intentional or accidental.

* A denial of service attack is when networked services are deliberately flooded with information to the point of collapse. An example would be overloading an email server with many hundreds of emails deliberately sent to the same address in a short space of time. An example of an accidental attack would be an Institute computer user sending an email with a very large attachment to every address in the Global address list. This would have an impact on the responsiveness of the service.

5.12 Backup and Restoration of Data

The Institute of Education has put into place systems to allow for the regular backup of and restoration of all data stored on its critical central IT infrastructure. The main purposes of the backup and restore system are as follows;

- To ensure that the Institute complies with and adheres to all current relevant legislation. This includes the Data Protection Act 1998, and the Freedom of Information Act 2000.
- Facilitate the recovery from major system failures to ensure that normal business operations can resume as soon as possible.
- The restoration of data that has become corrupt.

It is expressly not a user service offered for restoring users' files or folders that they have themselves accidentally deleted through error nor is to be used to restore individual or bulk email messages that have been accidentally deleted through user error or personal data. It is the responsibility of the user to take care when deleting, copying or moving important files, folders or email messages.

In extreme circumstances a request may be put forward to the helpdesk for data restoration. This request must come from a faculty manager or head of department directly.

5.13 Software Acquisition

The Institute needs to ensure that it is meeting responsibilities as a software user by ensuring that all multi user software acquired by the Institute is legal and appropriately accounted for. The Institute of Education is responsible for all software running on its network.

The Institute has a responsibility to ensure that the software installed is FAST Compliant (Federation Against Software Theft) and is installed in the correct way for the licensed number of users.

Software purchased using IOE resources, through IOE purchasing, remains the property of the Institute of Education. Licenses, media and documentation are not the property of end users and should remain with IS Computing for installation, reassignment and reuse as is appropriate.

Software purchased elsewhere may only be installed on the IOE Network or machines upon proof of appropriate license. Under this circumstance alone, users may retain the media and license (photocopy to ISC).

Below are the steps we need to take in order to ensure that all software purchased is processed into our inventory tracking system and all documentation of ownership is properly stored and maintained.

5.13.1 Steps in Acquiring Software

Work with IS to determine your software needs, the software package you wish to purchase and the resources that will be required in terms of hardware and security requirements.

IS will also be in a position to know whether the software is already available to you via existing spare licenses, or which is the most cost effective option to

Orders for software should be placed through IS, this avoids the wrong software/duplicate software being ordered and allows us to minimize the lead time required for installation. A budget code should be supplied

IS must be provided with a date when the software is required for use. If the software is for a major project such as a new Finance System this will be part of a project plan that IS is involved in. If it is software to be used by a small group, e.g. specialist teaching software for group of students, this information should be communicated via the Computer Helpdesk at least 6 weeks before the software is required.

When the item is delivered to IS, licensing information can be checked and entered in to the Definitive Software Library (DSL). The IT department retains media and documentation as needed to support our systems within the Definitive Software Library. Departments may keep copies of the original documentation for reference purposes.

After the check-in process is complete, IS will contact the requesting department to schedule software installation.

IS will require the following information for each employee who will receive the software:

- Name
- Email Address
- Phone Extension
- Machine Name/Number

If software needs to be reinstalled, contact IS to perform the reinstallation.

Copies of the End User License Agreement (EULA) and manuals will be made available to the department receiving the software.

If at any time an employee needs a copy of software documentation, the IT Department will provide it.

5.14 Prohibited Software

Users of computer systems connected to the Institute of Education's network are prohibited from running the following type of applications:

- software intended to subvert the security of any computer system, or seek vulnerabilities
- software intended to compromise any user's password or system password.
- software intended to intercept network traffic.
- software which has been obtained illegally or in breach of any licence agreement.
- P2P filesharing software or any applications that involve committing the Institute to sharing its network bandwidth in an uncontrolled and unlimited way e.g. Kazaa, BitTorrent, DirectConnect and Skype
- Applications that may introduce viruses or "spyware" when run.
- Download managers, such as GetRight
- HTTP tunnelling software

- Share scanning software, such as Sharescan, LANster