ENTERPRISE ARCHITECTURE WITH PLYMOUTH UNIVERSITY

Technology & Information Services

EA-ISP-009 - Use of Computers Policy

Owner:	Adrian Hollister
Author:	Paul Ferrier
Date:	26/06/2015
Document Security Level:	**PUBLIC**
Document Version:	1.01
Document Ref:	EA-ISP-009
Document Link:	http://blogs.plymouth.ac.uk/strategyandarchitecture/wp-content/uploads/sites/4/2015/06/EA-ISP-009-Use-of-Computers.pdf
Review Date:	June 2016

EA-ISP-009 - Use of Computers Policy

Document Control							
Version	**Author**	**Position**	**Details**	**Date/Time**	**Approved by**	**Position**	**Date/Time**
0.90	Paul Ferrier	Enterprise Security Architect	Created the document	12/02/2014			
0.91	Steve Furnell, Paul Dowland	Head of School of Computing and Mathematics, Associate Professor	Document review and comments	06/03/2014			
0.92	Paul Ferrier	Enterprise Security Architect	Revised in line with JANET AUP guidelines	03/10/2014			
0.93	Paul Ferrier	Enterprise Security Architect	Added user definition	19/01/2015 14:30			
0.94	Paul Ferrier	ESA	Altered policy to address the mobile environment more	19/06/2015 15:10			
1.00	PF, CD, PW, DM	ESA, EA, IT Director, Operations and Maintenance Manager	Final tweaks	26/06/2015 14:00	Paul Westmore	IT Director	26/06/2015 13:15
1.01	PF	ESA	Added a couple more references in	29/06/2015 10:00			

EA-ISP-009 - Use of Computers Policy

Introduction

The Use of Computers policy (that replaces the old 'Rules and Regulations of Computing Use') forms part of the University's Information Policy Set and should be read in conjunction with the Data Classification Policy (EIM-POL-001) as well as the Secure Working Policy (EA-ISP-014). The Use of Computers Policy sets out the responsibilities and required behaviours of all Plymouth University users of any information systems and includes: the information security aspects of acceptable use; good practice in the use of accounts and access credentials such as passwords (see Password Safeguarding below) and behaviour to protect against unknown or malicious code.

Definitions

Computer	is any type of electronic device that is capable of accessing or sending messages to another computer, which includes but is not limited to desktops, laptops, tablets, phablets and smart phones.
Password Safeguarding	refers to not disseminating your University account password to any other user, including Service Desk personnel. If access to your account is required to resolve a business problem, this should be performed with the end user present.
Restricted Data or Information	refers to either confidential, personal or sensitive personal information as denoted in the Data Classification Policy (EIM-POL-001).
University Network	refers to any connection for wired or wireless access to University resources including any downstream services (for example email, or digital learning environment when hosted by a third party)
User	is any person who is currently engaged in any form of study, employment or partnership with Plymouth University (including Academic Partnerships, Third Party Suppliers of Service), it also covers anyone who connects to the University Network (for example, connection to a free wireless network in a refectory) and finally it includes staff or students as part of their initial engagement with the University (for example from point of application for students or potential staff)

1. Safeguarding Equipment

1.1 Computers and other equipment, when in use that are used to directly access the University network must not be left unattended if they are logged in and unlocked (the only exceptions are open access kiosk devices and public display systems). Users must take all due care and attention when in open plan or unsecured locations, either by logging out of the device entirely or as an absolute minimum locking the screen before leaving the computer unattended.

1.2 Computers issued or owned by the University, when practical and where facilities exist, must be secured using Kensington locks or an appropriate locking mechanism when unattended.

1.3 Any computer that connects to the University network, in the future, will be required to meet a minimum set of standards including:

1.3.1 Anti-malware (both anti-virus and malware protection) installed, enabled and up-to-date

1.3.2 Operating system and application security patches released within the last thirty calendar days are installed

Failure of the computer to meet these standards will result in the device being quarantined on the network and may therefore not be able to access the required resources.

2. Files and Email

2.1 Electronic mail is inherently insecure, it must not be used to convey **restricted** information (please

refer to EA-ISP-007 Information Handling Policy[1] for further details) unless appropriate file encryption is used and the password is communicated through a different medium to the recipient, for example, a telephone call or an SMS.

2.2 Any information that is essential to the business that is created or stored (in a temporary capacity, as it must not be held there in the long term[2]) on a laptop or a computer's local hard drive must be copied to a suitably backed up University approved storage location at the earliest available opportunity. It is the responsibility of the user to ensure that this takes place on a regular basis.

2.3 **Restricted** information should generally only be accessed from equipment in non-public locations; if it is essential to access from a public location (for example, a café), then either:

2.3.1 All wireless communication methods should be disabled following retrieval of the required asset(s), or as an absolute minimum must not permit other users to gain access to the equipment without requiring a password;

2.3.2 Secure remote access controls must be established before the transmission of **restricted** files can begin. Guidelines for secure remote access are available for Windows[3] or Apple[4] computers.

2.3.3 Consideration must be given to any members of public and that are in close proximity to you when working in these environments.

2.4 For standard or restricted information, if printing of the material is permitted it must be printed on a network printer that does not default to immediate printing, for example in open plan offices.

2.5 When transporting files on removable media (specifically, but not limited to USB sticks, external hard drives), if the data is classified as restricted then the entire device or drive must be encrypted to prevent unauthorised disclosure if the device is lost or stolen.

2.6 The installation of software onto University owned or a leased computer is permitted, with the proviso that all licensing restrictions are adhered to. User installed software will not be maintained or supported beyond reasonable endeavours by Technology and Information Services; it may be removed if after investigation it is deemed to be obstructing the normal working of the core software on the device.

3. Appropriate use of services

3.1 It is understood that within the organisation a wide variety of disciplines and materials are created, distributed and consumed on computing devices; however, these materials must not fall into any of the categories detailed below (based on Janet's recommendations[5]), although this is not an exhaustive list:

- Any illegal activity
- Creation or transmission, or causing the transmission, of any offensive, obscene or indecent images, data or other material, or any data capable of being resolved into obscene or indecent images or materials.
- Creation or transmission of material with the intent to cause annoyance, inconvenience or needless anxiety.
- Creation or transmission of material with the intent to defraud.
- Creation or transmission of defamatory material or any such content that may bring the University into disrepute.
- Creation or transmission of material such that infringes the copyright of another person.
- Creation or transmission of unsolicited bulk or marketing material to users of networked facilities or services, save where that material is embedded within, or is otherwise part of, a service to

[1] EA-ISP-007 - (Information Handling Policy)
[2] EIM-POL-001 - (Information Classification Policy)
[3] SEC-GDL-002-1 - (Windows 7 & 8 Secure Connection Guidelines) University login required
[4] SEC-GDL-002-2 - (Mac OSX Secure Connection Guidelines) University login required
[5] JANET's AUP - https://community.ja.net/library/acceptable-use-policy

which the user or their organisation has chosen to subscribe.

- Deliberate unauthorised access to networked facilities or services.
- Deliberate or reckless activities having, with reasonable likelihood, any of the following characteristics:
  1. Wasting university staff effort, or Janet resources, including time on end systems on another university or college's network, and the effort of staff involved in the support of those systems;
  2. Corrupting or destroying other users' data;
  3. Violating the privacy of other users;
  4. Disrupting the work of others;
  5. Denying service to other users (for example, by overloading of access links or switching equipment, of University or Janet services, or of end systems on another university or college's network;
  6. Continuing to use an item of software or hardware after either the University or Janet Network Operations Centre (or its authorised representative) have requested that use cease because it is causing disruption to the correct functioning of the networking service;
  7. Other misuse of network resources, including the introduction of "viruses" or "malware" or other harmful software into the environment.
  8. Attempting to bypass security measures, such as but not limited to:
     - i Password capturing / cracking programs
     - ii Packet sniffing / analysing programs
     - Iii Port scanning
     - iv Using false (or spoofed) IP address or domain names
- Any network connected to the University's infrastructure that is being used to access another network, any breach of the acceptable use policy of that network will be regarded as unacceptable use.

3.2 Unless a business need has been identified and approved by either the Chief Information Officer (CIO) or an appropriate delegate within Technology and Information Services (TIS) all peer-to-peer traffic will be prohibited.

3.3 All users of the computing service must not permit information security safeguards and policies to be bypassed, or allow inappropriate levels of access to University information or IT facilities to other users or any third parties such as guests, customers, collaborators, suppliers, consultants and contractors.

3.4 For the provision of service that cover all areas of teaching and learning, it is necessary to share data with third parties, this will be dealt with in accordance with the Data Protection Act[6].

3.5 Where a computer has been provided by the University or one of its partners to a user for their work, when this device is no longer required it must be returned to Technology and Information Services' (TIS) Service Desk in its original state; for example, if the computer has been set up with personal credentials (as opposed to University issued credentials) these must either be provided or removed prior to the return of this computer.

3.6 All users of University services consumed on a computer will adhere to any pertinent Acceptable Usage Policy that covers the area of service provision (for example, the Halls of Residence Acceptable Usage Policy).

4. Monitoring of services

4.1 The University retains the right, at all times, to review, audit and restrict any and all information sent, received or transmitted on or through the network and any associated or connected devices to enforce the appropriate use of its services.

4.2 All activities or log information will be held in accordance with the retention requirements governed by

[6] Information Governance - Data Protection

the relevant statutory body.

4.3 The University will fulfil its obligations to comply with any requests from local or government jurisdictions, where evidence of a user or device information pertinent to investigations is required.

4.4 Where the acceptable use of any connection to the University network is being breached, throttling measures can and will be used to ensure that normal service is not degraded to other users.

Appendix

1. Safeguarding Equipment

Explanatory Notes

Computer equipment that has been logged on and unattended can present a tempting target for unscrupulous staff or third parties on the premises. However, all measures to make it secure should observe the organisation's access control policy.

2. Files and Email

Explanatory Notes

There are significant information security risks when receiving any files (including graphics files of any format), programs, or mobile code, etc. from the Internet.

There are many risks associated with transferring information by email, not the least of which is that it is normally sent in plain, readable text. It is vital that any information received is complete and correct and care is taken with electronically supplied data, such as email attachments, in case of possible forgery.

Essential data, wherever it is held, must be given adequate protection. Backing up data held on portable computing devices is a means to protect against its loss.

Accessing or printing restricted (including confidential) information in insecure locations increases the risk of the loss of documents sent to unattended printers.

Removable media, as the name suggests, are easily transportable and are often the primary means of data distribution. Their contents can often be read at most computers and, once copied onto the organisation's corporate network, the origin may be untraceable. Attention should also be given to the actions needed in the event that removable media is lost.

University owned or leased devices are primarily for corporate use, it is understood that benefit can be added by installing either apps on a mobile device, extensions to web browsers and other large applications. All of these applications must adhere to any licensing restrictions that are imposed as part of the installation or purchase of the software. If the computer is not functioning as expected and investigations are undertaken, if user added software can be attributed to the poor performance it may be required to remove this software, or the device be re-imaged or reset to factory defaults in the worst case scenario.

3. Appropriate use of services

Explanatory Notes

All users' of University services or connection to the University or partners network are required to be upholding the law in relation to their activities.

The University must be able to retrospectively disclose accurate information on request from the authorities regarding illegal activities and all points highlighted within section 3.1.

4. Monitoring of services

Explanatory Notes

In order to maintain a working service for all of the organisation's users it is important to know where problems may arise, before essential elements of service break. It is the intention for monitoring to be non-invasive of user activities, unless there is beyond reasonable doubt illegal or activities that are causing restrictions in service to other users.