ENTERPRISE
ARCHITECTURE
WITH
PLYMOUTH
UNIVERSITY

Technology & Information Services

EA-ISP-009 Use of Computers Policy

Owner:	Nick Sharratt
Author:	Paul Ferrier
Date:	28/03/2018
Document Security Level:	**PUBLIC**
Document Version:	1.05
Document Ref:	EA-ISP-009
Document Link:	
Review Date:	Mar 2019

Document Control							
Version	**Author**	**Position**	**Details**	**Date/Time**	**Approved by**	**Position**	**Date/Time**
0.90 – 0.94	Paul Ferrier	Enterprise Security Architect	Created the document	12/02/2014 – 19/06/2015			
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			
1.02	PF	ESA	Reviewed and revised policy	06/09/2017 16:30			
1.03	PF	ESA	Additional review	31/10/2017 09:45			
1.04	PF	ESA	Altered link for Classification Policy	02/02/2018 13:00			
1.05	PW, GB, NS, PF	IT Director, HoSM, 2x ESA	Updated prior to review	06/03/2018 12:05	Paul Westmore	IT Director	06/03/2018 17:20

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 Information Security 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 University of Plymouth 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

Device	is a collective term to describe a hardware component, irrespective of operating system that is used for transmitting, storing, accessing or manipulating university data, including (but not limited to) servers, laptops and desktop computers, smart phones, network switches and wireless access points.
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.
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 University of Plymouth (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 Devices 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. 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 Devices 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 University managed devices that connect to the University network, 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 applications updated regularly as per the Patching Policy[1]

2. Files and Email

2.1 Electronic mail is inherently insecure, it must not be used to convey **confidential** or **restricted** information (please refer to EA-ISP-007 Information Handling Policy[2] 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.

[1] https://www.plymouth.ac.uk/uploads/production/document/path/11/11252/SEC-POL-001-Patching-Policy.pdf

[2] https://www.plymouth.ac.uk/uploads/production/document/path/4/4053/EA-ISP-007-Information_Handling_Policy.pdf

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[3]) on a laptop or a computer's local hard drive must be copied to a suitable University approved storage location at the earliest available opportunity, such as Office365 (Team Site). It is the responsibility of the user to ensure that this takes place on a regular basis.

2.3 **Confidential** and **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 Secure remote access controls must be established before the transmission of **confidential** and **restricted** files can begin. For example, the use of a University virtual private network (VPN) being established on unsecured wireless networks.

2.3.2 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;

2.3.3 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 **confidential** 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, but requires the member of staff to authenticate to retrieve the print jobs.

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

2.6 The installation of software onto University owned or leased computers is permitted, with the proviso that:

2.6.1 it may remove the device from any compliance programme aimed at maintaining secure systems;

2.6.2 all licensing restrictions are adhered to;

2.6.3 the software will not be maintained or supported beyond reasonable endeavours by Technology and Information Services;

2.6.4 if the software is obstructing the normal operation of core software on the device it may be removed.

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[4]) unless approved by an ethical application, 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.

[3] EIM-POL-001 – https://www.plymouth.ac.uk/uploads/production/document/path/6/6015/EIM-POL-001_-_Information_Security_Classification_Policy_v1.1.pdf

[4] JANET's AUP – https://community.ja.net/library/acceptable-use-policy

- 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 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 Senior Information Risk Owner (SIRO) or a nominated 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 appropriate legislative or regulatory requirements.

3.5 Where a device 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 the 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 device 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 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.