FOI_15-064: response to question 2 & 6

Report Control Information

Title:	ICT Framework - Desktop Procurement and Deployment Policy
Date:	10th January 2011
Version:	V1.3
Reference:	ICT/POLICY/DSKCOMP-PROC/FINAL/V1.3
Authors:	Steve Mosley
Quality Assurance:	ISDMT

Attached is the Desktop Computer Procurement and Deployment Policy as approved by the Information Strategy and Services Committee (ISSC) on 4th February 2011.

Desktop Computer Procurement and Deployment Policy

Contents

Desktop Computer Procurement and Deployment Policy

Policy aim and scope

This document details Policy in regard to procurement and deployment of University owned desktop computer systems and the level of support that will be provided for this from Information Services. Recommendations and guidelines for best practice are also given in order to assist departments with their IT procurement strategies.

This Policy identifies and defines:

- University policy on preferred suppliers.
- Central procurement support.
- Policies regarding standard models.
- University policy regarding equipment replacement and disposal.

Policy monitoring and review

Information Services is responsible for the maintenance of this Policy. Any proposed revisions to the Policy will be discussed with Faculties, Central Divisions and the Purchasing Office prior to seeking approval from the Information Strategy and Services Committee (ISSC).

Policy

1. Suppliers

1.1 The Purchasing Office aided by Information Services will be responsible for determining preferred University suppliers for desktop computers, portable computers, printers and mobile devices utilising mobile phone technology (e.g. smart phones).

1.2 In determining University suppliers, the Purchasing Office will consult with Faculty IT support staff.

1.3 There will be no more than one supplier for each of the following categories:

- Desktop and portable PCs[1]
- Macintosh desktop (Mac) and portable computers (Macbook)[2]
- Mobile devices (e.g. smart phones) which use mobile telephone technology and which can be used to synchronise with UEA services such as email and calendars/diaries.
- Printers

[1] The term PC is an abbreviation for "personal computer" which is a term which covers all computers designed to be used by one person at a time. Branding has given a particular identity of "Mac" to PC products made by Apple. For the purpose of this document the term "PC" will be used to signify non-Apple products and the term "Mac" used for Apple products.

[2] Note: The UEA standard desktop and portable computer platform is the PC and Macs/Mac books should only be purchased in exceptional circumstances where a PC cannot meet requirements. Only PCs running the currently supported Windows operating system are supported as a desktop computing platform by Information Services and guaranteed to operate as clients for UEA corporate applications and services.

1.4 Wherever possible, University preferred suppliers will be a sub-set chosen from those awarded contracts on inter-regional/national university agreements.

1.5 All preferred suppliers will be published on the Purchasing Office Buyer's Guide web pages[3] on the intranet with contact details and information on how to purchase.

1.6 The Purchasing Office in consultation with Information Services and Faculties will proactively monitor the performance of contracts with suppliers, undertaking to identify and deal with issues and problems as they arise. An annual review of the contract will be undertaken by the Purchasing Office and regular liaison meetings arranged involving the supplier, Information Services and Faculties in order to facilitate information flow and to highlight and resolve any outstanding issues. Management information in support of the monitoring and review process will be arranged by the Purchasing Office with the supplier.

1.7 If a supplier's performance has been unacceptable, the Purchasing Office will inform them of such and will work with the supplier to identify the improvements that need to be implemented in order to achieve an acceptable level of service.

If a supplier's performance does not improve satisfactorily, the Purchasing Office will consult with Information Services and Faculties in order to decide whether and when to replace the supplier with a competitor chosen from the inter-regional/national supplier list.

1.8 A major review of each supplier will be undertaken by the Purchasing Office and Information Services every three years**.** Faculties will be consulted during this process. At this stage, current suppliers will either be confirmed or new suppliers chosen.

1.9 The Purchasing Office will ensure that any University purchasing arrangements with IT equipment suppliers are in compliance with existing and/or emerging government and European legislation**.**

1.10 The Purchasing Office, advised by Information Services will ensure via the tendering process that the sustainability and total cost of ownership of such computing equipment is taken account of, in particular, power consumption and disposal.

1.11 All departments will only purchase equipment from University preferred suppliers.

Exception

a. Where the University preferred suppliers cannot meet the equipment specification required for specialist research or teaching work.

b. Where equipment is connected to specialist scientific equipment and the supplier of that equipment determines the computer or printer supplier.

c. Where equipment is funded by an external agency which determines supplier.

1.12 Departments should purchase desktop and portable computers via the UEA Managed PC Procurement Service wherever possible – see 2.2.

1.13 All orders for desktop equipment of £20,000 or over should be checked with the Purchasing Office in order to ensure compliance with University policies and external legislation, and to ensure that appropriate measures have been taken to ensure that suppliers are offering a suitable level of additional discount in return for bulk purchasing.

[3] See https://www.uea.ac.uk/fin/buyersguide

2. Central procurement support

2.1 In addition to their role in determining and maintaining suppliers for personal computers, printers and mobile devices, the Purchasing Office will also determine and maintain a list of preferred suppliers for minor hardware (memory, disk drives etc) and consumables, selecting suppliers from those on inter-regional/national agreements where possible. They will consult with Information Services and Faculties in determining such.

2.2 The Purchasing Office assisted by Information Services will provide a Managed PC Procurement Service aiming to deliver cost effective (in terms of total cost of ownership) desktop systems which conform to University approved standards and policies regarding hardware, operating system and software. The service will demonstrate savings in purchasing overheads for departments and will provide a standard documented and supported standard process for procurement. Purchases from departments will be organised in such a manner as to obtain bulk purchase discounts which will be applied to all orders irrespective of volume.

3. Standard models

3.1 Information Services will provide via the Managed PC Procurement Service standard models for University owned desktop and portable computers. Standard Model PCs will be guaranteed to run UEA corporate applications and services effectively.

3.2 Departments are expected to select from these Standard Models as referred to in 3.1, except where there are specialist needs where greater computing power is required.

4. Deployment and Disposal

4.1 Faculties and Central Divisions should have a rolling replacement strategy for IT equipment, and build this into their budget setting process. This strategy should be approved by the Director of University Services and be in accordance with University approved IT and purchasing policies.

4.2 It is the University's aim to retain PCs for a minimum of 5 years, with appropriate migration of equipment between users and Schools/Units in order to achieve this aim. Replacement strategies for desktop and laptop computers should be consistent with this aim. After 5 years, a decision whether or not to retain the computer in service, or dispose of it should be made taking into account serviceability, fitness for purpose and total cost of ownership including power consumption.

4.3 Desktop and portable computers deployed should be in accordance with this Policy and the additional University policies[4] below:

- Desktop Computer Hardware Policy
- Desktop Computer Operating Systems Policy
- Desktop Computer Software Policy
- General Information Security Policy
- Security Manual

Justifiable exceptions are allowed, but should be in accordance with the exceptions and processes listed in the above policies.

4.4 At the end of their working life within the University, computers and printers should be disposed of using the disposal processes included in the Managed PC Procurement Service. Mobile devices

[4] See http://www.uea.ac.uk/is/itregs/ictpolicies for the policies

and other minor hardware whose disposal is not catered for by the Managed PC Procurement Service, should be disposed of using University approved processes. Redundant equipment should not be given or sold to staff or students at the end of its working life.

GISP17. IT and information asset management

Date:	8 November 2012
Version:	1.0
Authors:	Jonathan Colam-French
Quality Assurance:	Information Strategy and Services Committee (ISSC)

Version control

Revision	Date	Revision Description
1.0	8/11/12	Approved by ISSC

Policy

Security Control	Ensuring University IT and information assets are known, and access to these assets is managed.
Objective	• To ensure that the University is fully aware of all IT equipment and software assets it owns and there is a registered owner responsible for each asset. • To ensure that the University is fully aware of all information assets it owns and there is a registered owner responsible for each asset. • To ensure that migration and disposal of assets is managed according to defined procedures ensuring the University is compliant with financial regulations and relevant legislation. For information assets, see also the Information Classification and Data Management policy.
Policy	17.1. Inventories of all University owned IT and information assets will be maintained which includes an owner for that asset who is responsible for its day to day security. 17.2. Information assets should be classified according to the Information Classification and Data Management policy. 17.3. Disposal of assets at the end of their useful life within the University will be in accordance with University financial regulations and external legislation governing such. Disposal of computing hardware must be done in compliance with the University's policies regarding such (see Desktop Computer Procurement and Deployment Policy).
Responsibility	• Each Faculty or service unit is responsible for ensuring an inventory is in place for the assets it owns, and that the inventory is regularly reviewed to ensure that the records held remain accurate. • For departments where IT is managed by ITCS, it is responsibility of the ITCS managed IT technicians to maintain an up-to-date IT asset inventory for the department. • For other departments where the IT is not managed by ITCS, it is the responsibility of the department to maintain an up-to-date IT asset inventory for the department. • In either case, it is the responsibility of the department to maintain up-to-date inventories of the information assets it

	owns. - Those specified above who are responsible for the asset inventory will make this available to appropriate authorities within the University on request.
Incident Management	Where an information asset has been compromised, the owner of that asset should be notified. Further action is as defined by GISP14. Where an IT or information asset is not recorded in an inventory, the manager with responsibility for the asset should provide the IT Support Manager with appropriate details.

For more guidance on copyright see the web page at http://www.uea.ac.uk/is/strategies/infregs/copyright.

3.8 Software

a) Software is subject to copyright and licensing restrictions and persons involved in the illegal reproduction of software can be subject to civil damages and criminal penalties.

b) Software provided by the University should only be used in accordance with licence conditions of the software. You should not copy or distribute it to others unless authorised to do so.

c) In general, all users are expected to honour any agreements or contracts made by the University concerning any computer software or data that they use and to abide by the general principles as detailed in the Software Copyright Acknowledgement document which is available at http://www.uea.ac.uk/is/itregs/softwarecopyright.

d) Software Licence Agreements vary. The principal user of a single user system or the manager of a multi-user or networked system is responsible for the software loaded on that system and ensuring that it is used in accordance with the licence agreement.

e) Software provided by the University should not be deleted, disabled or altered, other than by authorised personnel.

f) Users must co-operate with persons employed by the University to carry out software and data audits, and where required follow software registration procedures.

g) Schools /Departments must keep an up-to-date inventory of all software installed on their computer systems and ensure that no software is installed for which the University does not have a current licence.

h) Schools/Departments must also ensure that any University licensed software is returned by leaving members of staff or students and any copies are removed from computers within their care, prior to leaving the University.

3.9 Computer security

a) All access to computers and the network should be authenticated by means of a Username and Password.

b) Strong passwords should be used following advice published at http://www.uea.ac.uk/password and complying with the University's password policies as defined in GISP5 of the General Information Security Policy at https://intranet.uea.ac.uk/is/strategies/infregs/infosec/GISP5. Passwords must be changed at least every 12 months to maintain security.

c) All IT equipment under the University's care should be maintained in a secure manner in accordance with the General Information Security Policy and Security Manual. IT support personnel have a particular responsibility in this regard.

GISP23. Mobile devices

Date:	8 November 2012
Version:	1.0
Authors:	Jonathan Colam-French
Quality Assurance:	Information Strategy and Services Committee (ISSC)

Version control

Revision	Date	Revision Description
1.0	8/11/12	Approved by ISSC

Policy

Security Control	Controls to minimise the risk of loss of University information assets when using mobile devices such as laptops, mobile phones, data sticks or removable storage or accessing University systems when off site and located at non-University premises.
Objective	To ensure that security is added to mobile devices to prevent unauthorised access and maintain confidentiality. To ensure that all information systems and assets are assessed as to their suitability for mobile or off site access before such access is granted.
Policy	23.1. Persons who will be doing part or all of their work using dedicated equipment in a fixed location outside the organisation (teleworking) must be authorised to do so by an appropriate authority within the organisation. A risk assessment based on the criticality of the information assets being used and the appropriateness of the proposed teleworking location should be carried out. 23.2. Teleworkers will be provided with appropriate computing and communications equipment and must use only this equipment for teleworking. The equipment provided may only be modified or replaced if this has been authorised. All equipment must be returned at the end of the teleworking arrangement, or when the teleworker leaves the organisation. 23.3. All teleworking agreements must include appropriate measures, based on a risk assessment, to protect the security of information assets. Teleworkers must follow the agreed security procedures at all times. 23.4. All teleworking agreements must include rules on the use of equipment provided for teleworking. Teleworkers must abide by these rules at all times unless specifically authorised. 23.5. Persons accessing information systems remotely to support business activities must be authorised to do so by their line manager or the system owner for the information system (as appropriate). A risk assessment based on the criticality of the information asset being used must be carried out. 23.6. Utmost care must be used when transporting files on removable media (e.g. disks, portable HDs, CD-ROMs and USB flash drives) to ensure that valid files are not overwritten and incorrect or out of date information is not

	imported. 23.7. The University will publish guidelines for users of mobile computing equipment advising them on how these should be used to conform to the information security policies and other good practices.
Responsibility	• Information Services is responsible for ensuring access to services by mobile devices is secured where possible, or unable to be accessed where no security option is available. • Information Services is responsible for providing guidance on good practice in the use of mobile devices. • Users are responsible for ensuring that their use of mobile devices or remote facilities is in accordance with good practice advice and the information security policies.
Incident Management	Incidents should be reported to the IT Helpdesk for further investigation.
Implementation	**Exchange mobile device security** An Exchange Security Policy should be applied to all mobile devices which synchronise with Exchange. The following settings for the policy should be applied: • Mobile device requires passcode • Minimum passcode length = 6 • Number of failed pass-code attempts until device is reset to factory default (formatted) = Maximum available[6] • Time without user input after which passcode must be re-entered (in minutes) = 5 • Enforce passcode history (remembers last 3 passcodes) • Require encryption on the storage card • Enable passcode recovery (user can obtain recovery passcode via OWA). • Enable a remote wipe facility for devices that synchronise to UEA email using ActiveSync. This can be used in the event that a device is lost or stolen and can be activated by the owner of the device through OWA. • In extreme circumstances, a remote wipe of a lost or stolen device can be performed by ISD but only with the explicit consent of the device owner. **Guidelines on use of mobile devices** Guidance on setting up security on a mobile device (phone or tablet) accessing the University email service is available from the Information Services web site at: https://intranet.uea.ac.uk/is/email/mobile-device-security.

[6] Maximum no. of failed attempts available = 16