**INFORMATION SECURITY POLICY - UNIVERSITY ADMINISTRATION AND SERVICES (UAS)**

*Updated 26 November 2013*

**SUMMARY**

*Part 1 – Aims and responsibilities*

* This policy supplements the University’s overarching information security policy and defines the framework within which information security will be managed across UAS.
* The aims of information security are to protect the availability, utility and confidentiality of information and to ensure compliance with legal requirements.
* The Registrar [HEAD OF UAS SECTION] is responsible for ensuring that UAS [NAME OF UAS SECTION] complies with this policy and all other university policies and procedures relating to information security.
* UAS [NAME OF UAS SECTION] shall protect the security of its information and information systems and use a risk-based approach to decide the appropriate level of control.
* UAS shall ensure that all users receive appropriate training and education in information security.

 Part 2 - *Procedures and practices*

* Mobile devices used to handle confidential information[[1]](#footnote-1)- laptops, tablets, smartphones, memory sticks, etc - must be appropriately secured. If they cannot be secured, they must not be used to handle confidential information.
* Users wishing to send confidential information via E-mail or cloud services such as OxFile, must ensure that documents are encrypted, using one of the approved methods in the Information Security Toolkit (the [‘Toolkit’](http://www.it.ox.ac.uk/infosec/protectyourself/documents/)).
* Confidential information should be stored on University managed servers and not on local hard drives.
* Confidential information should be downloaded from secure University systems (e.g. OSS, Oracle Financials, DARS) only when strictly necessary.
* Passwords must not be shared or easy to guess.
* Users must ensure that home computers used to access University systems are kept secure through firewalls, anti-virus software and security updates. Confidential University data should not be held on home computers.
* Files critical to the operation of UAS must be backed up.
* Confidential information should not be stored in e-mail folders.
* Envelopes containing confidential documents must be sealed securely and addressed correctly and, in the case of external mail, sent by recorded delivery.
* Confidential information must be removed from redundant or surplus IT equipment or office furniture before disposal.
* Appropriate physical measures must be taken to prevent the theft, loss or inadvertent exposure of confidential data e.g. lock computer screens when not at your desk, lock away hard copy confidential documents, do not read confidential information in a public place where it can be viewed by others.
* Any security incidents must be reported promptly- see section 17 below.

**This policy is divided into two parts.**

* **Part 1 deals with the broad objectives of information security and the division of responsibility between different groups within the department.**
* **Part 2 sets out the detailed procedures and practices that need to be followed by all end-users in order to implement the policy’s objectives.**

**Part 1 – OBJECTIVES AND ORGANISATION OF INFORMATION SECURITY**

**1. Roles and responsibilities**

The Registrar is ultimately responsible for the maintenance of this policy and for its implementation within UAS. This policy has been approved by the Registrar and senior officers and forms part of UAS’s policies and procedures.

The Registrar and senior officers are responsible for reviewing this policy on an annual basis. They will provide clear direction, visible support and promote information security through appropriate commitment and adequate resourcing.

Heads of UAS Sections are responsible for managing information security within their sections, in accordance with this policy, with appropriat**e** advice and guidance from IT Services. They may find it helpful to designate a deputy to assist them, who can act as the first point of contact on information security matters within the section.

It is the responsibility of all line managers within UAS to ensure that all staff for which they are responsible are 1) made fully aware of this policy; and 2) given appropriate support and resources to comply.

It is the responsibility of each user to comply with this policy, and with all other policies and procedures relating to information security. If a user is uncertain whether a particular activity is permissible under this or related policies, they should consult their line manager and/or head of section.

**2. Policy Statement**

UAS [NAME OF UAS SECTION] is committed to protecting the security of its information and information systems.

The information it manages must be appropriately secured to prevent breaches of confidentiality, failures of integrity or interruptions to the availability of that information, as well as to ensure appropriate compliance.

UAS shall provide education and training in information security and raise awareness of its importance. All UAS users must take the online training programme.

To determine the appropriate level of security control for information systems, a process of risk assessment[[2]](#footnote-2) shall be carried out in order to define security requirements and identify the probability and impact of security breaches.

Specialist advice on information security shall be made available throughout UAS and advice can be sought via the [University’s Information Security Team](http://www.ict.ox.ac.uk/infosec) and/or [OxCERT](http://www.oucs.ox.ac.uk/network./security).

**3. Importance of information security**

UAS’s computer and information systems underpin all UAS’ activities, and are essential to its objectives of supporting the University’s core academic purposes of teaching, learning and research; of ensuring the University can meet the requirements of government, funding bodies and other external agencies; and of facilitating the attainment of the objectives set out in the University’s Strategic Plan. UAS recognises the need for its staff, students, visitors and contractors to have access to the information they require in order to carry out their work and recognises the role of information security in enabling this. Security of information is essential to maintaining the continuity of its business activities and to its compliance with University regulations and policies.

**4 Purpose**

In July 2012, Council approved an information security policy that provides a general framework for the management of information security throughout the University. However, in order to accommodate local differences in security requirements, each department or unit is required to formulate its own information security policy.

This policy supplements the University’s overarching policy and defines the framework within which information security will be managed across UAS. It is the primary departmental policy under which all other technical and security related polices reside. **Annex A** provides a list of all other policies and procedures that support this policy. [*UAS sections to contribute relevant local policies and procedures, where applicable*]

**5 Scope**

This policy is applicable to and will be communicated to all users of UAS IT systems, including visitors and contractors. It covers, but is not limited to, any systems or data attached to UAS’s computer or telephone networks, any systems supplied by UAS, any communications sent to or from UAS and any data - which is owned either by the University or UAS - held on systems external to UAS’s network.

**Part 2 - DETAILED PROCEDURES AND PRACTICES**

This part is directed at end-users and sets out the procedures and practices they are expected to follow in order to implement the objectives identified in Part 1, particularly in relation to the protection of confidential information. The appropriateness of some procedures or practices will depend on local circumstances i.e. those at section level, and will need to be determined in the light of risk assessment. Where this is particularly the case, the procedure or practice has been marked with an asterisk\*. Any significant variations from this policy must be approved by the Head of Section and the reasons documented.

**6 Definition of confidential information**

In general, confidential information is any information that is not intended to be publicly available[[3]](#footnote-3). If the loss or unauthorised disclosure of information could have adverse consequences for the University or individuals, it is confidential.

Given the potentially serious consequences of breaching the Data Protection Act (DPA), you should assume that all personal data is confidential. (Personal data is any electronic or hard copy data that identifies a living individual e.g. a CV, email address, reference, job or course application, home contact details, etc.)

Examples of confidential information, involving both personal data and business information, are at **Annex B.**

**7. Training**

The Information Security Awareness training programme shall be taken by all permanent staff, all temporary staff employed for more than three months, and, where relevant, all consulting/internal staff working with UAS. New staff shall take the programme as part of their induction.

**8. Remote access and mobile devices**

*Remote Access*

Only trusted machines, not public kiosk machines, should be used to connect to the University network remotely.

Staff using personal computers (as opposed to University computers) to access University systems must protect University data by:

1. ensuring that the machine is protected by a firewall, anti-virus software and the installation of security updates;
2. using Citrix or another remote working service so that no University data resides on the machine; and
3. ensuring that the machine is encrypted, using one of the approved systems, if university data is to be downloaded to, or stored on, the machine.

*Mobile devices - General*

The use of mobile devices (laptops, USB/memory sticks, smart phones, tablets, etc) is an area of high risk, because they can be easily lost or stolen. It is essential that such devices be appropriately secured.

You must apply an appropriate password. Adjusting the default settings allows you to apply a more advanced password.

You should apply the latest security patches to your device.

When using your device on an unsecured public Wi-Fi network you must use the University’s Virtual Private Network (VPN) service (or similar local departmental service) in order to ensure a secure connection to the University network. Further information is available [here.](http://www.oucs.ox.ac.uk/network/vpn/)

Applications should be installed only from trusted locations.

*Laptops – University purchased*

University-purchased laptops must be protected through whole disk encryption (WDE), using the central service provided by IT Services. If there are exceptional operational reasons to justify the use of an alternative WDE technology, agreement for this must be sought from the head of section and the alternative technology must be implemented.

In a few cases, it may not be practicable or appropriate to apply WDE e.g. in the case of shared laptops, because of the number of users. In such cases, there must be an assessment of risk, and appropriate measures taken to reduce the risk and provide protection e.g. not using the laptop to store confidential information and/or keeping it in a secure room.

*Laptops – Personal*

UAS staff who use personal laptops to access University data must protect that data by using Citrix or another remote access service and by ensuring that the data is not downloaded to, or stored on, the laptop. If University data needs to be downloaded to, or stored on, a personal laptop, the data must be protected by encrypting the laptop, using one of the approved systems listed [here](http://www.it.ox.ac.uk/infosec/wde/).

(These requirements also apply to personal desktops – see ‘Remote Access’ above.)

*Other devices (Tablets, Smartphones, Blackberrys)*

There is a range of ways to secure other devices and if the device is to be used to handle confidential information, it must be appropriately secured, in accordance with the advice given [here](http://www.it.ox.ac.uk/infosec/istoolkit/useofmobiledevices/#d.en.116185.). If this cannot be done, you must not use the device to hold or transmit confidential data.

*Memory sticks*

Memory sticks used to hold confidential University data must be encrypted, using AES 128 bit encryption or better. Advice on obtaining encrypted memory sticks should be sought from IT Support staff.

**8 Information Exchange (including Email and Cloud Services)**

*E-mail*

Please take extra care and precautions with confidential data, and only email such data if it is (a) absolutely necessary and (b) safe to do so. If the risks are high, consider alternatives to email: Weblearn or Sharepoint. Or encrypt the file, by using one of the methods described in the [Toolkit](http://www.it.ox.ac.uk/infosec/protectyourself/documents/) (7-zip is the preferred method, and is available from the standard Oxford application installer).

You must ensure that emails containing confidential data are sent to the correct address and not rely solely on any ‘autocomplete’ function. You should take particular care when selecting an address from a directory.

If you receive confidential information inadvertently via e-mail, you should delete it as soon as possible[[4]](#footnote-4).

Confidential information should not be stored in e-mail folders, as it is not secure. If an e-mail or e-mail attachment contains information that needs to be kept, you should save it to a secure area of the network.

*Cloud Services*

\*You must obtain explicit authorisation from the information owner for the storing, exchanging or synching of confidential information in order to ensure that any such activity is secure. The information owner may need to seek advice from the Information Security Team in IT Services.\* The University provides its own private cloud services and these should be considered ahead of public services. Further information is [here.](http://www.oucs.ox.ac.uk/sis/cloud/)

*Hard copies*

When sending confidential data by fax, you must ensure you use the correct number and that the recipient is near to the machine at the other end ready to collect the information immediately it is printed.

When sending confidential documents by post, whether internal or external post, you must ensure that the envelope is sealed securely, marked ‘Private and confidential’, and addressed correctly. Recorded delivery must be used for confidential documents sent by external post.

**9 Storage**

Confidential data should be stored on University managed servers and not on local hard drives.

\* Where an additional layer of security is required for data stored on University servers, confidential data must be password protected or encrypted.\*

**10 Access**

Approval to access confidential information shall be granted at an appropriate level, recorded, and reviewed regularly. [To access [*Secure Storage/Confidential Information*], you must obtain explicit authorisation from [*Role*].\*

Having access to a shared drive does not imply that you have permission to view all the folders/files on that drive. You should view only the information you need to carry out your work.

You must not under any circumstances share your password with others or allow others to use your account to access the department’s network or other resources.

Passwords should not be easy to guess. Further guidance is [here.](http://www.oucs.ox.ac.uk/registration/index.xml?ID=passwords)

**12 Copying data and working off-site**

\*Confidential data must not be copied without the permission of the information owner.\*

To avoid the risks of taking copies of confidential information off-site, you should as far as possible use remote access facilities to look at confidential information held on University systems.

Confidential data should be downloaded from a secure system (e.g. OSS, Oracle Financials, DARS) only where permitted by the rules that apply to that system.

You must ensure that any copies you make of confidential data are the minimum required and that they are deleted or destroyed when no longer needed.

**13 Backup**

Any files critical to the operation of UAS must be backed up; if you are unsure whether this is being done, seek advice from your local IT support staff.

Before confidential data is encrypted, you must ensure that any critical data is securely backed-up.

You must ensure that mobile devices containing back-up copies of critical data are securely stored (see section 15 below on physical security).

**14 Disposal**

When disposing of surplus or obsolete mobile devices containing confidential data, you must ensure that any confidential data is removed permanently from the device (deleting the visible files is not sufficient).

You must remove any files or papers before disposing of old office furniture.

Confidential documents must be shredded when no longer needed.

**15 Physical Security**

You must lock your workstation, laptop or tablet when leaving your desk and log out when leaving for the day.

Confidential information data must be stored in a locked cupboard, cabinet or drawer. If this is not possible, you must lock the room when it is unoccupied for any significant length of time.

Keys to cupboards, drawers or cabinets must not be left on open display when the room is unoccupied.

When travelling with a mobile device, you must take reasonable care to reduce the risk of loss or theft.

You should not read confidential data in areas where it can be easily viewed by others.

**16 Software**

\* Each UAS Section should determine the extent to which their staff members are able to download software onto their computers, and under what circumstances local IT support staff or Section heads must be consulted before this is done.\*

**17 Reporting**

Suspected or actual security incidents e.g. the theft or loss of a mobile device, a virus attack, should be reported immediately to OXCert and your line manager, who will consult with the head of section, as appropriate.

The section [*Unit Name*] shall keep a record of all security incidents and follow the University’s advice for the escalation and reporting of such incidents. Further information is here. Incidents involving personal data shall be reported to the University’s Data Protection Team.

**18 Enforcement**

Any failure to comply with this policy may result in disciplinary action.

**ANNEX A**

**University –wide policies**

Information security policy - <http://www.it.ox.ac.uk/infosec/ispolicy/>

Regulations and Policies applying to all users of University ICT facilities - <http://www.ict.ox.ac.uk/oxford/rules/>

**Policies applicable to UAS Section**

[UAS SECTION TO SPECIFY]

**ANNEX B**

**Examples of confidential information**

The following list consists of generic examples and is for the purpose of illustration only. UAS Sections may wish to replace or supplement them with examples specific to their circumstances.

**Examples of Personal data[[5]](#footnote-5)**

1. Any set of data that could be used for fraud or identity theft, including but not limited to bank account or credit card details, national insurance number, passport number, home address, date of birth.
2. Data relating to an individual’s application for a job, performance in a job interview, work performance, promotion or disciplinary record
3. Data relating to a student’s academic performance or disciplinary record
4. Data relating to an individual’s personal or family life e.g. their interests, hobbies, relationships
5. Any sensitive personal data, as defined in the DPA i.e. information relating to:
* health (mental or physical),including disability
* ethnicity or race
* sexual life
* trade union membership
* political opinions
* religious beliefs
* commission or alleged commission of a criminal offences
* criminal proceedings

**Examples of Business information**

1. Information provided to the University on the understanding that it is confidential, whether explicit or assumed
2. Information the disclosure of which would disadvantage the University’s position in negotiations, whether commercial or otherwise
3. Reorganisation or restructuring proposals that would have a significant impact on individuals, prior to a decision being announced
4. Exam questions before the examination takes place
5. Security arrangements for buildings or for high profile visitors or events
6. Papers discussing proposed changes to policies or procedures on high profile or sensitive issues, before the changes are announced

1. See definition of ‘confidential’ in section 6 below [↑](#footnote-ref-1)
2. See section 4 of University policy: [↑](#footnote-ref-2)
3. See section 6 of University ISP for a more detailed definition [↑](#footnote-ref-3)
4. To remove it permanently, you must also delete it from your deleted items folder. [↑](#footnote-ref-4)
5. Any recorded information, hard copy or electronic, which identifies a living individual e.g. name, e-mail address, reference, CV, photograph. [↑](#footnote-ref-5)