PHYSICS DEPARTMENT INFORMATION SECURITY POLICY

SUMMARY

Part 1 – Aims and responsibilities

- The aims of information security are to protect the availability, utility and confidentiality of information and to ensure compliance with legal requirements.

- The Head of Department is responsible for ensuring that the Physics Department complies with this policy and all other university policies and procedures relating to information security.

- The Physics Department shall protect the security of its information and information systems and use a risk-based approach to decide the appropriate level of control.

- The Physics Department 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 - laptops, tablets, smartphones, memory sticks, etc - must be appropriately secured. If they cannot be secured, they must not be used to handle confidential information.

- Owners of confidential data should regularly review whether there is any ongoing need to retain the data. In cases where there is a long term need, it may be sufficient to store the data in anonymised form.

- Users are required to take appropriate steps to safeguard confidentiality whenever exchanging information with others. This applies to all forms of data communication including email, printed documents, fax, letter, cloud services etc. If a user is unsure of the appropriate method and safeguards to use to exchange some specific confidential data, they must refer to the data owner for a decision.

- Confidential information should be stored on departmentally managed IT systems within home directories or managed file shares and not on local hard drives. The Department will ensure that these are physically secured, regularly backed up and that access is controlled appropriately.

- Confidential information should be downloaded from secure University systems (e.g. SITS, Oracle Financials, DARS) only when strictly necessary.

- Passwords must not be shared or easy to guess.

- Home computers used to access University systems must be kept secure through firewalls, anti-virus software and security updates. It is recommended that that any work involving confidential data is performed by remote login to Physics department servers. This avoids moving a copy of the data to the home computer.

- Critical files must be backed up. The department backs up data stored in home directories on a daily basis.

- Envelopes containing confidential documents must be sealed securely and addressed correctly and, in the case of external mail, sent by recorded delivery.

- Redundant or surplus IT equipment should be disposed of through the departmental IT services who will ensure that confidential material is removed. Office furniture must also be checked before disposal.

- Appropriate physical measures must be taken to prevent the theft, loss or inadvertent exposure of confidential data e.g. if others have access to your office you should lock computer screens and lock away hard copy confidential documents before leaving the room. Do not read confidential information in a public place where it can be viewed by others.

- Any security incidents must be reported promptly.

PHYSICS DEPARTMENT INFORMATION SECURITY POLICY

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 Policy Statement

The Physics Department is committed to protecting the security of its information and information systems.

The information it manages shall 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.

The Physics Department shall provide education and training in information security and raise awareness of its importance.

To determine the appropriate level of security control that should be applied to information systems, a process of risk assessment 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 the Physics Department and advice can be sought via the University's Information Security Team.

2 Importance of information security

The Physics Department's computer and information systems underpin almost all departmental activities, and are essential to the research, teaching and administrative processes of the department. The Physics Department 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.

3 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 the Physics Department. It is the primary departmental policy under which all other technical and security related polices reside.

4 Scope

This policy is applicable to and will be communicated to all departmental members and other relevant parties who use Physics Department IT systems and services (e.g. visitors, conference guests, contractors etc*).* It covers, but is not limited to, any systems or data attached to the Physics Department's computer or telephone networks, any systems supplied by the Physics Department any communications sent to or from the Physics Department and any data - which is owned either by the University or the Physics department - held on systems external to the Physics department's network.

5 Roles and responsibilities

The Head of Department is ultimately responsible for the maintenance of this policy and for its implementation within the Physics Department. This policy has been approved by the Physics Management Committee (PMC) and forms part of its policies and procedures.

The PMC 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.

The Senior Administrator is responsible for the management of information security and, specifically, to provide advice and guidance on the implementation of this policy.

The Information Security Advisory Group comprising representatives from all relevant sections of the Physics department is responsible for identifying and assessing security requirements and risks. Current membership of the group can be viewed at (URL to be added).

It is the responsibility of all line managers within the Physics Department to ensure that all staff for which they are responsible are 1) made fully aware of the 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, IT manager or senior administrator (who make seek further advice and guidance as required).

Part 2 - DETAILED PROCEDURES AND PRACTICES

This part is directed at end-users and sets out the procedures and practices you need 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 the results of the department's risk assessment.

The following sections cover various areas where awareness of Information Security best practice is essential. The department will aim to provide information systems which support best practice so that those handling confidential data can do so as efficiently as possible.

6 Definition of confidential information

For this purpose, confidential information is any information that is not intended to be publicly available. If the loss or unauthorised disclosure of information could have adverse consequences for the University or individuals, it is confidential. Examples of what should be considered confidential data is given in Appendix A.

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 data that identifies a living individual e.g. a CV, email address, reference, job or course application, home contact details, etc.). When processing of confidential data has been completed, the data should be removed from all systems or the data anonymised if appropriate.

We understand that guidance for retention of student data is being prepared by University administration and until this is available we should continue with the current policy that student data should be self-anonymised after one year.

The Senior Administrator must be notified of all sources (databases, files, printed documents) containing confidential information so that the risks can be discussed and entries made in the risk register.

7 Use of 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 are 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 VPN service (or similar departmental services) in order to ensure a secure connection to the University network. Further information is available here.

Applications should be installed only from trusted locations.

If available, enable a facility to allow remote wiping of the device should it become lost or stolen.

Encryption of laptops and USB/memory sticks

Any laptop or USB/memory stick containing confidential data must be encrypted, using AES 128 bit encryption or stronger. In practice, it is likely that most people will hold some confidential data (e.g. email caches, personal bank account details, login credentials etc) on their mobile devices so encryption should be used wherever possible.

Other devices (Tablets, Smartphones, Blackberrys)

There are 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 principles stated in the IS toolkit. If this cannot be done, you must not use the device to hold or transmit confidential data.

8 Information Exchange (including Email and Cloud Services)

E-mail

Sending an email is like sending a postcard in the mail. There is no built-in confidentiality (or 'envelope') to prevent anyone who 'handles' the message from reading it. Connection to the University mail servers is protected by encryption in the form of SSL/TLS and this is the case for most other service providers. However once an email leaves the University's network it should be assumed there is no protection. Since an email you send may be routed via anywhere in the world, and a copy of the email will be stored at each step along the way, it is best to start from the basic principle that you shouldn't put anything in an email that you wouldn't want to be made public.

You should first consider communicating confidential information by a more secure method than e-mail. If a suitable alternative is not available, you should consider encrypting the message and/or attachment. Further information is available here. If you are not sure on the appropriate way to exchange some confidential data, you should take advice from the data owner.

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.

When you receive confidential information by email you should consider what steps you can take to safeguard it (e.g. by removing sensitive parts to more secure storage such as your home area). If it is only of short term use, then the message should be flagged or moved to another folder for later review.

Cloud Services

You must obtain explicit authorisation from the IT manager for the storing, exchanging or synching of confidential information in order to ensure that any such activity is secure. The University provides its own cloud services and these should be considered ahead of public services. Further information is here.

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.

When printing confidential documents always check that the destination printer is correct, do not rely on default settings. Consider using hold queues (e.g. SHARPHOLD) which require a login at the physical printer before printing starts.

9 Storage

There are many advantages to storing confidential data on departmentally managed IT systems rather than mobile devices. You may also wish to consider password protection or encryption for such data. Advice can be obtained from the IT manager. In some cases, it may be appropriate to audit all accesses to confidential data and this can be discussed with the IT manager.

10 Access

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. Access controls will generally be set following requests from line managers and will be based on role and need.

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.

11 Remote Access

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

Home computers used for remote access must be appropriately protected, typically by a firewall, anti-virus software and by the installation of security updates. It is recommended that that any work involving confidential data is performed by remote login to Physics department servers. This avoids moving a copy of the data to the home computer.

12 Copying and working off-site

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 when strictly necessary.

You should 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 critical files must be backed up. The department backs up files stored in home folders and other folders by arrangement. Separate arrangements need to be made if backups are required of large volumes of data. Anyone, who is uncertain about backup arrangements for their data should consult their local IT officer or the departmental IT manager, Before confidential data is encrypted, you must ensure that any critical data is securely backed-up.

If a user is running backups to their own storage devices (e.g. time-machine) the backups should be encrypted. Any storage which may contain unencrypted copies of confidential data should be disposed of through the departmental IT services.

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 devices containing confidential data, you must ensure that any confidential data is removed permanently from the device (deleting the visible files is not sufficient). This should be done via the departmental IT support staff. This includes all devices with some element of internal storage including desktops, mobile devices, servers, network storage devices etc.

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 if leaving them where others may have access.

Confidential 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

Software installation on departmentally managed systems is usually performed by IT staff or through self-service facilities. Users requiring additional software should consult with IT staff.

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 itsupport@physics.ox.ac.uk. Such incidents will then be tracked by the ticketing system and investigated as appropriate.

The Physics Department shall keep a record of all security incidents and follow the University's advice for the escalation and reporting of such incidents. 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

Supporting Policies and Procedures

http://www.it.ox.ac.uk/policies-and-guidelines. Regulations and Policies applying to all users of University ICT facilities. These apply to all staff, University and other relevant parties, including visitors and contractors.

ANNEX B

Examples of confidential information

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

Examples of Personal data[1]

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] Any recorded information, hard copy or electronic, which identifies a living individual e.g. name, e-mail address, reference, CV, photograph.