# Table of Contents

1. Introduction .................................................................................................................. 2
   1.1. The purpose of this Procedure ................................................................................. 2
   1.2. Scope of this Procedure ......................................................................................... 2
2. Compliance ....................................................................................................................... 2
3. Data Confidentiality Levels ............................................................................................. 2
   3.1. Introduction ............................................................................................................. 2
   3.2. Information Classification ...................................................................................... 3
   3.3. Access to personal data ......................................................................................... 3
4. Personal Computer Security ............................................................................................ 3
   4.1. Passwords ............................................................................................................... 3
   4.2. Securing your computer when you are away from your desk ................................ 5
5. Security While Off-Campus ............................................................................................. 6
   5.1. Purchasing Portable Computers, Smartphones, PDAs .......................................... 6
   5.2. Notebook Security .................................................................................................. 6
   5.3. Software Security ................................................................................................... 6
   5.4. Virus Protection ...................................................................................................... 6
   5.5. Password Security .................................................................................................. 7
   5.6. Losses and Confidentiality/Security Breaches ......................................................... 7
   5.7. Off-campus access to data ..................................................................................... 7
6. Equipment and Data Disposal .......................................................................................... 8
   6.1. Disposal of equipment or data ............................................................................... 8
   6.2. Disposal procedure ................................................................................................. 8
7. Systems Security ............................................................................................................... 9
   7.1. Access to business systems .................................................................................... 9
   7.2. Access by non-University members ....................................................................... 9
   7.3. System backups ...................................................................................................... 9
   7.4. Change management procedures .......................................................................... 9
   7.5. Terrorism Act 2006 ............................................................................................... 10
   7.6. Event log auditing .................................................................................................. 10
8. Security and Third-Parties ............................................................................................... 10
   8.1. Confidentiality declaration ..................................................................................... 10
9. Network Security .............................................................................................................. 10
   9.1. Attachment of servers to the network ................................................................. 10
   9.2. Firewall access procedures ................................................................................... 13
   9.3. Wireless authentication procedure ....................................................................... 14
   9.4. Modem attachment ............................................................................................... 15
   9.5. Unauthorised monitoring ...................................................................................... 15
10. Appendix A. Confidentiality Declaration .................................................................... 16
11. Appendix B. Data Protection Statement ..................................................................... 17
1. Introduction

1.1. The purpose of this Procedure
The I.T. Security Procedure Manual is designed to be used in conjunction with the University of Huddersfield I.T. Security Policy.

It gives practical advice to members of the University and describes procedures that must be followed in order to implement the provisions of the I.T. Security Policy.

This document will be updated regularly in the light of the security threats we face and as the technological environment changes.

1.2. Scope of this Procedure
This Procedure applies to all I.T.-related equipment, processes and data that belong to the University of Huddersfield, or is managed on its behalf, wherever accessed.

2. Compliance
All members of the University, affiliates and third-parties will comply with this I.T. Security Procedure and, where appropriate, their compliance will be monitored.

3. Data Confidentiality Levels

3.1. Introduction
The security procedures that are appropriately applied to a given set of information will depend on the characteristics of that information. It is important, therefore, to have an easy-to-understand information classification scheme that indicates the level of protection that must be applied.
3.2. Information Classification

<table>
<thead>
<tr>
<th>Access</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sensitive</td>
<td>To be accessed by a strictly controlled group of users, with owner’s consent, and with highest security levels applied. Not to be passed on without consent. Subject to the Data Protection Act.</td>
</tr>
<tr>
<td>Confidential</td>
<td>To be kept secure and accessed only for business need. To be passed to third parties only as required for the fulfilment of the University’s contract with the individual, except with permission. Subject to Data Protection Act.</td>
</tr>
<tr>
<td>General</td>
<td>Not restricted</td>
</tr>
</tbody>
</table>

3.3. Access to personal data

It is important that those staff who, as part of their system management or troubleshooting roles, have access to personal or individual data understand the implications of the Data Protection Act and how it affects them. For further information on the University’s Data Protection Policy see:

http://www.hud.ac.uk/sec/data_protection.html

All staff who are likely to have access to such data must sign a confidentiality declaration, which is retained by the School or Service. A pro-forma is given in Appendix B.

4. Personal Computer Security

4.1. Passwords

Passwords are the key to many systems and applications. A password helps to prove identity, and to ensure personal privacy and helps to protect the privacy of the data being accessed. Poor passwords compromise security. Passwords must comply with the advice in the following sections.
4.1.1. Good Passwords
A good password is one that is difficult to guess. It will use a wide range of characters in an unpredictable order. A good password is one that can be remembered easily and typed in quickly so that anyone looking over your shoulder will not be able to see what you are typing.

A password must;
- be at least seven, preferably eight, characters long
- contain a mixture of letters, numbers and punctuation
- not appear in any dictionary or any other list
- have no personal connection with the owner

**example:** Sg2MgVSgMx (the first letter of each word of a line of a song or poem, with punctuation and numbers added)

4.1.2. Bad Passwords
A bad password is simply one that is easy to guess, or so difficult to remember that the owner writes it down.

A password must not;
- be blank, or obvious, such as 'letmein', 'opensesame', or 'password'
- be less than seven, preferably eight, characters long
- be written down, left in an open drawer, or pinned to a monitor
- contain simple sequences of letters or numbers such as qwerty, or 123456, or the reverse of a simple sequence
- contain a phone number or date
- be based on a nearby object at the time of choosing, such as 'monitor', or 'keyboard'
- appear in a dictionary (in any language) or any other list
- have a personal connection with the owner such as a car registration or pet's name.

**examples:** Ule4G (too short), Csb1-016 (room number), 0143aikon (product name reversed)

4.1.3. Changing passwords:
Passwords must be regularly changed, but not so often that they cannot be remembered

4.1.4. Safeguarding passwords:
- if a password must be written down, it must be kept in a secure location; alternatively, hints could be written down and not the password itself
- passwords must not be disclosed to anyone else, except perhaps a system administrator who needs it in order to solve a problem. If a password has been revealed, it must be changed immediately
- passwords must not be stored on a computer, PDA or mobile phone. The "save my password" feature must never be used
- passwords must never be sent by email, unless the message is encrypted
- computers left unattended must be logged off or have their keyboard locked
- public computers such as a cybercafé or lab PCs, must be shut down and restarted after use.
4.2. Securing your computer when you are away from your desk.

When a computer is left unattended, it is essential that that no unauthorised person can gain access to it.

There are a number of simple techniques that should be used.

- **Log out.**
  This will prevent any access until a valid username and password is entered.

- **Lock the keyboard.**
  To do this, press `Alt` and the `L` key at the same time.

To unlock the computer, use the Ctrl Alt and Del keys and re-enter your usual login password. Your computer will resume from the point at which you locked it.

- **Use a password-protected screensaver.**
  A screensaver with password-protection can be set to activate after a certain number of minutes of keyboard inactivity. To do this, right-click on a blank part of the Windows desktop area and choose **Properties**. Choose the **Screen Saver** tab to display the following screen;

  ![Screen Saver Properties](image)

  Select a screensaver using the drop-down arrow, select a number of minutes to wait until it activates and put a tick in the **On resume, password protect** box, then click **OK**. After the specified number of minutes of keyboard inactivity, the screensaver will activate. To remove it, you will need to re-enter your usual login password and your computer will resume at the point at which the screensaver activated.
5. Security While Off-Campus

5.1. Purchasing Portable Computers, Smartphones, PDAs.
There are several additional checks that must be performed when a mobile data-carrying device (such as a notebook, smartphone or PDA) is purchased.

It is the responsibility of the person arranging the purchase, e.g. the Client Consultant or local technician, to find out if the customer intends to use the portable device to hold sensitive or confidential data.

Any data must be stored in such a way that it can easily be backed up or identified for encryption. Any data of value to the organisation must be placed on secure institutional storage such as the SAN on return to campus. Client Consultants will advise on the best way to achieve this.

If sensitive or confidential data is to be stored, suitable security management tools must be employed – for example, by using a secure USB memory stick. Advice can be obtained from a Client Consultant.

5.2. Notebook Security
Users of University-owned notebooks must follow these guidelines:

Notebooks must be treated as carefully as if they were the user’s own property.

Notebook security is the responsibility of the user.

Notebooks must be securely locked away when not in use and must not be left unattended in a public place.

If a notebook securing cable is used, one key must be kept with the owner and another in a secure separate location.

Notebooks must be locked away in the car boot and not left on view inside a vehicle.

Notebooks must not be left within sight of ground floor windows or within easy access of external doors.

5.3. Software Security
Users of University-owned notebooks must not install any unapproved software. This applies to software downloaded from the Internet, unlicensed or illegal software, or software obtained from any other source.

Advice on installing additional licensed software can be obtained from a Client Consultant or local technical staff.
5.4. Virus Protection
University-owned notebooks must have approved security software which includes, as a minimum, anti-virus and anti-spyware components.

The anti-virus software’s database of virus definitions must be updated regularly, each day preferably, but at least once a week.

If a virus is discovered it must be reported immediately to Staff I.T. Support (01484 473737).

5.5. Password Security
All portable computing devices (such as a notebook, smartphone, or PDA) that contains University information must be password protected.

In addition to the general guidelines given in Section 4 concerning passwords, the following additional provisions apply to devices intended for use off-campus.

- Passwords must not be displayed on screens as they are entered.
- When allocated a new/temporary password for start-up use by the system’s manager/administrator the user must immediately change it.
- Passwords must be changed on change of staff or staff resignation.
- A boot up password must be used if this feature is available.

Where sensitive or confidential data is to be kept on the device the use of encryption software or a hardware device is mandatory in order to protect the data if the device is lost or stolen.

5.6. Losses and Confidentiality/Security Breaches
All incidents which result in a loss of hardware or where data security is compromised, must be reported directly to the University Security Manager. If sensitive or confidential information is involved, the person with responsibility for the data, such as the Director of Financial Services, must be informed immediately so that an assessment of the required action can be undertaken.

The University Security Manager will investigate the incident and establish the nature and potential security threat resulting from it.

Reportable incidents include, but are not limited to:

- Loss/theft of hardware.
- Loss/theft of software/data.
- Unauthorised access.
- Misuse of system/privileges.
- Illegal software download.

5.7. Off-campus access to data
When accessing data via the off-campus access connection whether at home, on another user’s PC or in a public place, users must ensure that:

- sensitive or confidential information is secured by the use of passwords or file encryption
6. Equipment and Data Disposal

The University has introduced an environmentally-responsible procedure for the disposal of all electrical and electronic equipment. In relation to the disposal of I.T. equipment, a secure data erasure procedure has been integrated into the process.

6.1. Disposal of equipment or data.
This procedure applies to PCs, printers, hard drives, interface cards, notebooks, PDAs, external hard drives, USB memory sticks and memory cards and any other devices that may potentially contain data.

Data on hard drives, USB memory sticks and memory cards could potentially contain sensitive or confidential data and must never be thrown away in bins or skips. The risk is reduced if secure USB memory sticks are employed for sensitive or confidential data.

6.2. Disposal procedure
Contact the Repair Service (ext. 2027) in Computing & Library Services to register your equipment collection.

Stickers will be issued to label each piece of equipment or box of parts. The School/Service must enter the following details on the labels.

```
Sample Label
C & LS AUTHORISED DISPOSAL

HUBS
Cost Centre.............
```

Arrange for Campus Support to take the labelled equipment to the central pick up point. Equipment without a sticker will not be removed.

All materials that are not re-usable will be disposed of in an environmentally-approved manner.

All hard drives, USB memory sticks and memory cards will be erased to the required standard and if not re-usable will be physically destroyed.

Computing & Library Services will retain all documentation related to the disposal.
7. Systems Security

7.1. Access to business systems
Authorisation to use any of the University's business applications must be requested from the system owner by the applicant's line manager. For example, the line manager of someone needing to use Agresso should contact Financial Services' Help Desk by email or in writing to request the required access level. If approved, Financial Services will create the account. They may require the prospective user to undertake some basic training prior to enabling use of the live system.

Requests for access to ASIS are handled differently due to the organisational structure surrounding ASIS. Authorisation is granted by the ASIS Director in response to a completed ‘Request for New User’ form. The prospective user must sign a separate Data Protection declaration and undertake training before being given access to the system. For staff in schools, requests to the ASIS Director will normally be channelled via the School ASIS Manager.

Anyone unsure of the procedure for obtaining authorisation to use any other application should contact Staff I.T. Support on 3737.

7.2. Access by non-University members
The University has established the Affiliates Procedure for handling the granting of I.T. privileges to those who have a relationship with the University but who are not employed by it. All requests for affiliate access must use the procedure detailed on the Computing & Library Services website: http://www.hud.ac.uk/cls/affiliates

7.3. System backups
System backups play an important role in ensuring business continuity in the event of an I.T. equipment or software failure by providing a method of restoring systems to pre-failure state.

When designing system backups a number of factors must be taken into consideration such as the rate at which system data changes and the length of time tolerable for the system to be out of operation. In essence, a system backup must be designed to capture all information required to restore the system to a working state as quickly as possible and to a point at which a minimum amount of data or transactions have been lost.

For major University systems such as email, Blackboard, student records, SAN home directories and many others, system backups are performed by Computing & Library Services, however there are many other I.T. systems which are managed at a local level by Schools and Services for which system backups must be performed by local staff.

Data stored on the SAN is backed up centrally, but Computing and Library Services does not carry out system backups that capture data stored locally on PCs (for example on C: or D: drives), notebooks or other personal devices. Backup for data on these devices must be carried out by their owners.

7.4. Change management procedures
Changes made to systems under the management of Computing & Library Services must be governed by the agreed departmental change management procedure. Systems not under the management of Computing & Library Services must also use a change management procedure appropriate to the importance of the data to the University.
Advice on a suitable process can be obtained from the Chair of the Infrastructure Review Group in Computing & Library Services.

7.5. Terrorism Act 2006
Following notification by the Police of material which may contravene the Act, the University has two working days in which to remove the offending web pages.

Owners of web servers delivering pages to the web or intranet will be required to provide details of the servers to the University webmaster in Computing & Library Services, plus contact information for at least two people who manage the web content of those servers. This must include any web services delivered on behalf of the University outside the University network, e.g. by broadband connections.

To comply with the Act, system owners will be given one hour during normal working hours to remove notified material, or the server will be shut down. Outside normal working hours the Computing & Library Services Senior Management Team will arrange for the server to be shut down at the earliest convenience.

7.6. Event log auditing
System audit logs must be created and maintained as appropriate to the importance of the system to the University.

System audit logs must be discussed with system owners to identify those areas of business systems which must be subject to audit logging to preserve the integrity of data.

Logs for both UNIX and Windows server-based business systems must be reviewed each week.

Logs for network logon/logoff, telephone traffic and web page access must be kept for at least 12 months.

8. Security and Third-Parties

8.1. Confidentiality declaration
Where the risk to sensitive or confidential data is deemed sufficient, the University requires that third-parties, such as suppliers who need to access such data, will be required to sign a confidentiality declaration using the pro-forma in Appendix A.

9. Network Security

9.1. Attachment of servers to the network
The attachment of a server to the network brings with it a number of security considerations. These are focussed on the data the server contains and the people who are going to access it. For these reasons, both the server and the network need to be protected.

9.1.1. Attaching a new server to the campus network
Prior to a new server being purchased, discussion with the Client Consultant responsible for your School/Service must take place and the following issues addressed to certify a secure connection, before the purchase can go ahead.

- Does this server replace an existing server? If so, please also refer to the procedure for **Removal of a server from the campus network**.
- Will the server provide data or applications?
- Will the server be for staff, student or other use?
- Will access to the server be required on or off campus, or both?
- What server operating system will be used?
- What applications will be used?
- Can the service required be hosted on an existing server?
- Where will the server be located – building and room no. - is the environment suitable (temperature, humidity, power & data)?
- Will technical support for the server be provided by the School/Service or by Computing & Library Services?
- What is the predicted growth of any data on server?
- What is the backup and recovery strategy for the server?
- What is the whole life cost of server, backup solution, software and maintenance?

The server must then be purchased through your Client Consultant who will act as liaison between yourself and the relevant teams within Computing & Library Services. After the server has been delivered to the chosen location you will need to contact your Client Consultant and provide them with the following:

- Proposed Server name
- Inventory and Serial numbers
- MAC address of the network card that is to be attached to the campus network
- UTP wall point to which the server is to be connected

This information is required so that we can provide you with the necessary IP network address/es and helps us to maintain an accurate record of server provision.

You will then be contacted by DHCP Admin who will provide you with the IP address/es for the server. You are then in a position to begin building the server in accordance with the current Computing & Library Services best-practice guide for your specified operating system. If you need any further advice on how to build the server or need someone from Computing & Library Services to build it for you, then please contact your Client Consultant who can arrange this.

Please note that Computing & Library Services reserves the right to disconnect any server from the campus network which does not conform to this procedure until such time as it is compliant and ceases to pose a security risk.

### 9.1.2. Attaching an existing server to the campus network

Prior to a server being attached to the network, discussions with the Client Consultant responsible for your School/Service must take place and the following issues addressed before the attachment can go ahead.

- Will the server provide data or applications?
- Will the server be for staff, student or other use?
- Will access to the server be required on or off campus, or both?
- What server operating system will be used?
• What applications will be used?
• Can the service required be hosted on an existing server?
• Where will the server be located – building and room no. - is the environment suitable (temperature, humidity, power & data)?
• Will technical support for the server be provided by the School/Service or by Computing & Library Services?
• What is the predicted growth of any data on server?
• What is backup and recovery strategy for the server?
• What is the whole life cost of server, backup solution, software and maintenance?

In addition you will also need to provide your Client Consultant with the following:

• The machine’s existing host name and most recent location, building and UTP wall point number.
• Proposed Server name
• Inventory and Serial Number
• MAC address of the network card that is to be attached to the campus network
• UTP wall point to which the server is to be connected

This information is required so that we can provide you with the necessary IP network address/es and helps us to maintain an accurate record of server provision.

You will then be contacted by DHCP Admin who will provide you with the IP address/es for the server.

Please note that Computing & Library Services reserves the right to disconnect any server from the campus network which does not conform to this procedure until such time as it is compliant and ceases to pose a security risk.

9.1.3. Renaming a server on the campus network
Prior to a server being renamed, please email DHCP Admin with the following information:

• Old server name
• Inventory and serial number
• IP Address/es
• MAC address
• New server name
• Location – building, room number and UTP wall point number. If the server is being moved to a new location, previous location details must also be provided
• Reason for change.

DHCP Admin will then record the information and ensure your request is passed quickly to the Client Consultant responsible for your School/Service who will then act as liaison between yourself and the relevant teams within Computing & Library Services.

Please note that Computing & Library Services reserves the right to disconnect any server from the campus network which does not conform to this procedure until such time as it is compliant and ceases to pose a security risk.
9.1.4. Removing a server from the campus network

Prior to a server being removed, please email DHCP Admin with the following information:

- Server name
- Inventory and serial number
- IP Address/es
- MAC address
- Location – building, room number and UTP wall point number.
- Reason for removal. If the server is to be replaced, please also refer to procedure for attaching a new server.

DHCP Admin will then record the information and ensure your request is passed quickly to the Client Consultant responsible for your School/Service who will then act as liaison between yourself and the relevant teams within Computing & Library Services.

9.2. Firewall access procedures

In order to maintain an appropriate level of information security, the University of Huddersfield’s computer network is separated from the Internet by a network firewall. For many of the University’s business systems to operate it is necessary to allow network traffic to pass through this firewall on an incoming and/or outgoing basis using a series of network ‘port’ numbers.

As there are many network ports which are commonly used by a variety of systems and where these are deemed to provide little or no risk to the University’s information security, these are routinely configured as ‘open ports’ within the firewall. However, on occasion there may be a requirement for a system to use a network port which is not routinely open. In these instances it is necessary to undertake an assessment of the business need and associated risk factors prior to the port being opened in the firewall.

*The procedure below describes how this must be done for clients outside Computing & Library Services.*

A request for opening ports in the firewall must be made in the first instance to the appropriate Client Consultant.

The Client Consultant will then obtain full details of the service being requested and who will require access to it including the following specific details :-

- A list of port numbers
- Whether traffic on these port numbers is required on an internal or external basis and whether the traffic is single or bi-directional
- MAC & IP address of the device/s for which port access is required.
- The preferred date from which access is desired. If access is only required for a limited period, then an end date must also be provided.

The Client Consultant will then email this information to the Network team mailbox for assessment.

The Network team will carry out an assessment of the request based on a combination of security best-practice and existing University of Huddersfield security policies.
If, on the basis of the information provided, the Network team approves the request, the Client Consultant will receive confirmation via email.

The Network team will implement the change and maintain a record of firewall access which has been approved through this procedure.

If, on the basis of the information provided, the Network team is unable to approve the request, then the Client Consultant will be asked to arrange a discussion between the client and the Network team in order to obtain further information, additional authorisation, or an alternative approach.

Where additional authorisation is felt to be necessary, this will need to be provided by the appropriate Head of Department or School Dean in the form of a written Service Level Agreement to be drafted by the Client Consultant.

The Network team will also maintain a record for access requests which have not been approved.

The procedure below describes how this must be done for clients within Computing & Library Services.

A request for opening ports in the firewall must be made to the Network team mailbox. The request must include full details of the service being requested and who will require access to it including the following specific details:

- A list of port numbers
- Whether traffic on these port numbers is required on an internal or external basis and whether the traffic is single or bi-directional
- MAC & IP address of the device/s for which port access is required.
- The preferred date from which access is desired. If access is only required for a limited period, then an end date must also be provided.

The Network team will carry out an assessment of the request based on a combination of security best-practice and existing University of Huddersfield security policies.

If, on the basis of the information provided, the request is approved, the Network team will implement the change and maintain a record of firewall access which has been approved through this procedure.

If, on the basis of the information provided, the Network team is unable to approve the request, then the request will be forwarded to the Head of C&IT for approval in writing.

The Network team will also maintain a record for access requests which have not been approved.

9.3. Wireless authentication procedure

Although providing many opportunities for more flexible use of I.T., wireless technologies are, in general, inherently insecure and therefore use of them on campus needs to be strictly controlled and monitored to ensure appropriate levels of security and regulatory compliance.
Only wireless networks that have been approved by Computing & Library Services will be permitted.

Any unauthorised wireless networks will be disconnected from the campus network without notice.

Authorisation to participate in the development of wireless networks can be sought via Client Consultancy.

User’s own equipment can be connected to the University wireless network provided that it meets the required standards, and subject to acceptance of the University Regulations Governing the Use of Computing Facilities.

9.4. Modem attachment

A modem is an electronic device that connects computers via a telephone line, allowing the exchange of information over the line. They are most commonly found in conjunction with fax machines, dial-up connections to banking or payroll facilities and servers which have remote access support arrangements with external suppliers.

Unless secured properly, such as by the use of dial-back, modems represent a potential security threat to the University’s I.T. systems, therefore their use and configuration must be authorised by Computing & Library Services.

Any unauthorised modem connections which are identified will be disconnected from the campus network without notice.

Authorisation to install a device with a modem can be sought via Client Consultancy who will liaise on your behalf with Telephone Services.

9.5. Unauthorised monitoring

The use or provision of tools which allow the monitoring of network traffic ("sniffing") is not allowed. Those who believe that they have a legitimate business need to use such tools (for example in teaching) should contact the Head of C&IT in Computing and Library Services to discuss how this can be carried out with due regard to the relevant legislation and without breaching the personal security of network users.
10. Appendix A. Confidentiality Declaration

The University of Huddersfield.

CONFIDENTIALITY DECLARATION

OUTSOURCING AND THIRD PARTY ACCESS TO UNIVERSITY I.T. SYSTEMS

<Insert organisational details here>

<organisation name> undertakes to the University of Huddersfield that it shall (and shall procure that its employees, agents and sub-contractors shall):

a. keep confidential all information of a confidential nature (whether written or oral) that it obtains or receives as a result of the discussions leading up to, entering into, or performance of, any contract with, or let by, the University (the “Information”);

b. not without the prior written consent of the University disclose the Information either in whole or in part to any other person save those of its employees, agents and sub-contractors involved in the implementation or evaluation of the contract who have a need to know the same for the performance of their duties;

c. use the Information solely in connection with the implementation or evaluation of the contract and not otherwise for its own benefit or the benefit of any third party.

Provisions (a), (b) and (c) above shall not apply to the whole or any part of the Information to the extent that it can be shown by <organisation name> to be:

i. known to <organisation name> prior to the date entered below and not obtained directly or indirectly from any other party; or

ii. obtained from a third party who lawfully possesses such Information which has not been obtained in breach of a duty of confidence owed to the University; or

iii. in the public domain in the form in which it is possessed by the University other than as a result of a breach of a duty of confidence owed to the University; or

iv. required to be disclosed by legal process, law or regulatory authority.

Signed on behalf of <organisation name>

Name: _______________________________________
Signature: _____________________________________
Date: ____________________

Approved by UTLC 19th July 2007
minor updates March 2009 & September 2009
Appendix B. Data Protection Statement

ACCESS TO PERSONAL OR INDIVIDUAL DATA

It is important that those staff who, as part of their system management or troubleshooting roles, have access to personal or individual data understand the implications of the Data Protection Act and how it affects them.

Under the terms of the Act, access to personal or individual data should be restricted to those data items which are necessary in order to perform system management or troubleshooting duties.

Additionally, data must not be disclosed to a third party without the express consent of the data subject or owner. In practice this means that documents, information, or the means to access them, should not be given to other members of the University or to external individuals or agencies, including the police, unless in exceptional circumstances; see below.

Staff should not use any additional access privileges granted to them to view or obtain confidential information relating to their own role(s) within the University, either as staff or student, which would not normally be available to them. Where any such access is likely to occur in the performance of a system management or similar task, staff should consult their line manager before proceeding.

In certain exceptional circumstances, personal or individual data may be given to a third party, for example to assist the police in a criminal investigation but only on production of a formal documented request.

A list of staff members designated to deal with police enquiries can be found at:

http://

A line manager may request access to the data stored in an absent employee's individual storage area, in order to assist the operation of the University, such as to retrieve lecture notes or assessment material required urgently.

Staff should also be aware of the consequences of accessing data beyond that which is necessary, or of disclosing personal or individual data without permission. In certain cases this could lead to disciplinary action or prosecution of the individual by the Information Commissioner.

Any queries regarding what information may or may not be accessed or disclosed should be addressed to the University Secretary.

. For further information on the University’s Data Protection Policy see:

http://www.hud.ac.uk/sec/data_protection.html

I understand the implications of the Data Protection Act as outlined above.

Name: ........................................................................................................................................

School/Service: ...........................................................................................................................

Signature: ....................................................................................................................................

Date: ........................................................................................................................................