

Acceptable Use Policy

1	General	2
1.1	Introduction	2
1.2	Definitions	2
1.3	Effective Date of this Acceptable Use Policy	3
1.4	Scope of this Acceptable Use Policy	3
2	UWTSD-Owned ICT Hardware.....	3
3	UWTSD-Owned Software	4
4	Personally-Owned Software.....	5
5	UWTSD Campus LAN	5
5.1	Accounts.....	6
5.2	Passwords.....	6
5.3	File store and E-mail servers.....	6
5.4	Accountability	7
5.5	Data Protection	7
5.6	Other UWTSD Servers.....	7
5.7	Other Network Items	7
6	Internal and External E-mail	8
6.1	Etiquette.....	8
6.2	Defamation	10
6.3	Discrimination & Harassment	10
6.4	Contractual Liabilities	10
6.5	Disclaimers	11
6.6	Viruses in e-mail.....	11
6.7	E-mails sent to Staff that contain suspected child pornography	12
6.8	Out of Office Auto-replies	13
6.9	UWTSD e-mail accounts	13
7	Internet Use	14
7.1	JANET AUP	14
7.2	Intellectual Property Rights and Copyright	14
7.3	Downloading	15
8	Behaviour	15
8.1	Offensive Material.....	15
8.2	General behaviour	16
9	Equipment not owned by UWTSD	16
9.1	Student PCs in Halls of Residence	16
9.2	JANET Roaming Service	17
9.3	Other Equipment used on campus.....	17
10	Wireless Connectivity	18
11	Monitoring	18
12	Disciplinary Measures.....	19
12.1	All Users	19
12.2	Penalties for Staff	19
12.3	Penalties for Students or Visitors.....	19
13	Absent Staff	20
13.1	E-mail sent to Absent Staff	20
13.2	Files of Absent Staff	20
14	Leavers	21
14.1	Staff	21
14.2	Students.....	22
14.3	E-mail Forwarding.....	22

Acceptable Use Policy

1 General

1.1 Introduction

The use of networked Personal Computers (PCs) as a work tool, a research tool and a communications tool has become essential in modern times. Today, nearly all office-based employees in the western world have access to a personal computer with e-mail facilities, and many of those have always-on Internet access as well. This certainly describes the staff and students here at UWTSD, many of whom could not function without ready access to computing facilities, especially e-mail and the Internet.

To meet this need, UWTSD invests substantial sums of money each year in ICT equipment and software for the benefit of all staff and students.

This document:

- sets out permissible uses of any ICT equipment and software supplied by *or used on* UWTSD premises, including but not limited to PCs and printers, the UWTSD LAN, all central servers, e-mail facilities and the Internet;
- specifies the prohibited uses of the above;
- states what monitoring will take place;
- sets out acceptable online behaviour;
- stipulates unauthorised access areas, in terms of both UWTSD facilities and on the Internet;
- sets out privacy rules in relation to other Users;
- sets out privacy rules in relation to UWTSD's right to monitor; and
- stipulates possible disciplinary consequences for a breach of these rules.

1.2 Definitions

AUP	Acceptable Use Policy
Disclaimer	A short piece of text added to an e-mail for legal reasons
ICT	Information and Communications Technology
Junk e-mail	See SPAM
JANET	Joint Academic Network, owned and run by JANET (UK)
JANET(UK)	Formerly UKERNA. The organisation which runs JANET on behalf of the JISC
JISC	Joint Information Services Committee of the UK post-16 and Higher Education Funding Councils
LAN	Local Area Network
SPAM	Unwanted commercial e-mail or hoaxes
Staff	All employees of UWTSD, both academic and non-academic
Technician	A suitably qualified, competent and experienced member of staff whose Job Description includes working on ICT Hardware or Software
UCS	Information Services (Formerly University Computing Service, Lampeter)
NS	Information Services (Formerly Network Services, Carmarthen)

Acceptable Use Policy

Server	Any computer offering resources over a network
Users	All users of computing facilities of UWTSD, be they staff, student, or a visitor with temporary access privileges
UWTSD	University of Wales Trinity Saint David

1.3 *Effective Date of this Acceptable Use Policy*

This document is effective for the Academic year 2011/12 and until rescinded or superseded. It should be reviewed at least annually, or more frequently as changing circumstances dictate.

1.4 *Scope of this Acceptable Use Policy*

This Acceptable Use Policy applies without exception to all Users of computing facilities of UWTSD, be they staff, student, or a visitor with temporary access privileges, and whether registered as a User with Information Services or not.

It covers Users' activities while using any computing facilities owned by UWTSD wherever those facilities may be located (e.g. a UWTSD Laptop Computer taken home).

It covers Users' activities while using any other computing facilities used on the UWTSD campus, including personally owned PCs in Halls of residence.

It covers Users of UWTSD facilities who have connected from off campus to access UWTSD resources.

All Users will be deemed to be familiar with and bound by this AUP, copies of which are on the UWTSD Website and Intranet Site, in all common workrooms, in all departmental offices, in the Students Union and in the Library.

2 UWTSD-Owned ICT Hardware

The definition of UWTSD-Owned ICT Hardware covers all physical items of ICT equipment, including but not limited to:

- Cables
- Desktop Personal Computers
- Digital Cameras
- Digitising Tablets
- Headphones
- Laptop or Notebook Personal Computers
- LCD Projectors
- Mice, Keyboards and Monitors
- Modems.
- Network Cabinets
- Network Sockets and Cables
- Personal Digital Assistants (PDAs)

Acceptable Use Policy

- Printers
- Scanners
- Servers
- Speakers
- Switches and Routers
- Tablet Personal Computers
- Video Conferencing Equipment
- Video Recorders

These items are supplied by UWTSD for academic and academic-related purposes. They may be freely used for these purposes, for limited personal use (but see 'JANET AUP' on Page 14 and also 'Internal and External E-mail' on page 8) and for any other use expressly approved by the Head of Information Services, but they may not be used for any other purpose.

In the main, computing facilities should not be used by staff for personal or private use unrelated to legitimate university activities. Limited and appropriate personal use that complies with the University of Wales, UWTSD Acceptable Use Policy is permitted, but only before or after your contracted hours or during recognised work breaks. Employees may be disciplined for wasting work time if they engage in the personal use of computing facilities when they should be attending to their duties. Staff should seek permission from their managers for any personal use of computing facilities that falls outside of this guidance. Staff are reminded that their terms and conditions of employment also restrict what is and what is not a permitted use of UWTSD facilities.

Only Technicians may service, modify, add or remove components or in any other way alter the ICT equipment belonging to UWTSD.

No User may modify, expose the inner workings of, connect extra peripherals to or in any other way tamper with any item of ICT Hardware without the express written consent of the Head of Information Services.

As regards the very popular USB 'Pen Drives', they are a peripheral in many senses. However, these devices are identical in function to a floppy disk as far as what they can have on them is concerned. Therefore, all users may freely use such devices to transfer files to and fro as long as their use complies with this AUP in all other respects, with the Information Security Policy and with the Data Protection Act.

No User should relocate any item of ICT Hardware, other than items such as Laptop computers that are intended to be portable. Relocations should only be carried out by Technicians.

3 UWTSD-Owned Software

The definition of UWTSD-Owned Software covers all programs licensed in the name of UWTSD. This includes but is not limited to:

- Operating Systems

Acceptable Use Policy

- Productivity Software, e.g. MicroSoft Office
- E-mail software
- Installed Freeware and Plug-ins.

These items are supplied by UWTSD for academic and academic-related purposes. They may be freely used for these purposes, for limited personal use and for any other use expressly approved by the Head of Information Services in writing (but see 'JANET AUP' on Page 14 and also 'Internal and External E-mail' on page 8). They may not be used for any other purpose.

Staff are reminded that their terms and conditions of employment also have a bearing on what is and what is not permitted use of UWTSD facilities.

Only Technicians or other Users who have obtained the express written consent of the Head of Information Services may install, configure or uninstall any software on UWTSD-owned hardware.

4 Personally-Owned Software

The definition of Personally-Owned Software covers all software programs licensed in the name of any User.

Such software will not normally be approved for installation on UWTSD-owned Hardware.

In exceptional circumstances, and subject to:

- the User having a justifiable need for the use of this software in their academic work;
- the production of a valid licence expressly permitting the installation of the software on more than one PC (it will always be assumed that the User has already installed one copy of the software on a personally owned PC);
- the production of original media;
- in the case of a member of staff, their line manager approves the request and is unable to purchase a licence for the software due to it no longer being on sale;

The Head of Information Services may approve the installation of such software.

Information Services will normally retain the original media and license documentation for the period that such software is installed on UWTSD-owned hardware.

Only Technicians or other Users who have obtained the express written consent of the Head of Information Services may install, configure or uninstall any software on UWTSD-owned hardware.

5 UWTSD Campus LAN

Acceptable Use Policy

Access to central file servers, e-mail facilities and the Internet is all accomplished by means of networking. Virtually all PCs on campus are networked together on the campus LAN and thus, by traversing JANET, to the Internet. Given this connectivity, inappropriate or offensive actions of any individual on our network reflect badly on UWTSD as an institution.

Information Services therefore has the ability to track the actions of any computing User on campus, in order that we can detect and put a stop to any wrongdoing (see 'Monitoring' on page 18).

No equipment of any sort may be connected to the campus LAN without the prior consent of the Head of Information Services.

Only Technicians or other specifically designated and approved persons may carry out such connections.

5.1 *Accounts*

Each User is allocated a unique logon name. By means of the username and password presented when logging on to the network at any PC, the Network Servers uniquely identify that specific User and ensure that they can access their own e-mail account and centrally stored files, plus any other resources they are allowed to use.

5.2 *Passwords*

Passwords are crucial to the security of the network, so the longer and more complex they are and the more frequently changed, the better. Unfortunately that can also make them harder to remember, which is why so many people base their passwords on easy to guess information like children's names, telephone numbers, car registration, date of birth etc.

Information Services can offer guidance on creating secure but memorable passwords easily.

Passwords should

- be at least 8 characters in length
- never be divulged to anyone else
- be changed regularly.

The UWTSD Information Security Policy (see <http://intranet.UWTSD.ac.uk/pdf/policies/InformationSecurityPolicy2009-10.pdf>) addresses this issue in more detail.

5.3 *File store and E-mail servers*

Users are all allocated an area on central servers for file and e-mail storage.

Acceptable Use Policy

In the case of staff, the space allocated to them is not limited at the moment, though in practise few staff should need more than one gigabyte.

Shared storage areas for use by staff of individual departments are unlimited in size.

In the case of students, Undergraduates are allocated 40MB and Postgraduates are allocated 100MB. All students are allocated a further 20MB quota for storage of e-mails on the e-mail servers. Students of IT-related subjects are given larger limits by Information Services by arrangement with the relevant academic department.

Users may access their file store from any networked PC on campus, or by means of the CITRIX system, whether in student halls or via the Internet.

Users may access their UWTSD e-mail account from any computer anywhere in the world with an internet connection and suitable web browser.

5.4 *Accountability*

Under no circumstances should you allow anyone else to log on to the network using your username and password. Users are responsible for any actions on the network attributed to their network account. All Users should take care to log off any PC properly when leaving it unattended, to prevent unauthorised access or impersonation.

5.5 *Data Protection*

If employees/students are required to put information (including photographs) onto the University's system containing personal data other than their own, the express written consent of the individual to whom the personal data relates must have been obtained.

The University of Wales UWTSD Data Protection Guidelines March 2004, should be consulted for further information. This can be seen at <http://www.UWTSD.ac.uk/policies/pdf/dp-handbook-march2004.pdf>

5.6 *Other UWTSD Servers*

Several other specialised servers exist on the network. You have no right to access any server on the UWTSD campus LAN unless you are specifically informed of your right to do so by the Administrator of that server.

5.7 *Other Network Items*

You have no right to attempt to access any other users' files, the network equipment itself, or indeed anything other than the facilities expressly granted to you when you registered. Any attempt to do so will be logged and the User will be disciplined.

Acceptable Use Policy

6 Internal and External E-mail

6.1 *Etiquette*

E-mail is a useful tool, but like many tools, it can be abused.

The following tips are intended as helpful guidelines rather than rigid rules, but should be followed when sending any e-mails, whether purely internal (i.e. to a xxx@tsd.ac.uk address) or external.

6.1.1 General

- Don't keep mail longer than necessary, especially with large attachments.
- Do include a brief signature on your e-mail messages to help the recipient understand who it is from.
- Don't use an over-elaborate signature on your e-mail message. Never, ever, use scanned images in a signature as these tend to be very large.
- Don't send excessive multiple postings to people who have no interest. This is known as "spamming" and is considered to be ignorant.
- Don't forward chain letters or "make money fast" messages. There are several hoaxes about to do with viruses - never pass these on without checking with Information Services first.
- Don't mark things as urgent if they aren't, because then when you really do have an urgent message it may not be treated in the way it deserves.
- Do not reply to SPAM, ever. It tells the sender that the address they sent that particular message to is 'live', and you will then start to receive even more SPAM. Clicking on any 'Remove me from your lists' links does exactly the same thing. The best thing to do with SPAM is to delete it unread.

6.1.2 Writing Style

- Do try to think about the message content before you send it out.
- Do be polite. Terseness can be misinterpreted.
- Do try to use humour and irony sparingly. You can use smileys such as :) or :(to indicate facial expressions, but make sure that the recipient understands what they mean.
- Do try to quote from the original message where relevant. You can break the quoted message down into paragraphs and comment on them individually to make it clearer.
- Do use emphasis where it's useful to do so. A common convention is to use a *star* either side of the word you want to stress.
- Don't type in CAPITALS as this is considered to be SHOUTING. This is one of the rudest things you can do in e-mail.
- Don't over-use punctuation such as exclamation marks ("!!") as these are meant to be for emphasis. In particular avoid more than one exclamation mark ("!!!"), especially if your e-mail is quite formal. Also, over-use of the full-stop (e.g. "....") can make a message difficult to read.

Acceptable Use Policy

- Don't criticise people's spelling, it is considered petty. Many people have no way of running a spell check on their messages and we all make typos.

6.1.3 Composing or Replying to e-mails

- Make sure you use 'Reply' and 'Reply to all' correctly.
- Do ensure that you have a relevant "Subject" line. Leaving the subject line blank may well result in the recipient just deleting your e-mail without reading it.
- Do tell your correspondent if you forward a message to somebody else to deal with, so they know who to expect a reply from.
- Don't copy out an entire, long message just to add a line or two of text such as "I agree".
- Don't "flame" people by sending them abusive e-mail messages.
- Don't make personal remarks about third parties. E-mail messages can come back to haunt you.

6.1.4 Suitability

- Don't reply to an e-mail message when angry, as you may regret it later. Once the message has been sent you will not be able to stop it being delivered.
- Don't say in an e-mail something you would hesitate to say to the recipient's face.
- Don't send unsuitable e-mail or attachments that you would hesitate to send in a memo or letter, especially anything of a sexual nature.
- Don't send anything that must stay confidential in an unencrypted e-mail. Use encryption or send a letter instead.

6.1.5 Attachments

- Do remember to tell people the format of any attachments you send if they're anything other than basic Microsoft Office file types.
- Don't send people large attachments unless you are sure they want to receive them.
- Remember attachments can contain viruses. Don't forward them unless you know they are clean.

6.1.6 E-mail Discussion Lists

- Do be patient, especially with inexperienced e-mail users. Give people the benefit of the doubt - just because you are familiar with e-mail etiquette, it doesn't mean that they are.
- Do be careful when replying to mailing list messages, or to messages sent to many recipients. Are you sure you want to reply to the whole list?
- Don't send irrelevant, off-topic messages.
- Don't criticise people's spelling, it is considered petty. Many people have no way of running a spell check on their messages and we all make typos.
- Don't conduct arguments in public.
- Don't "flame" people by sending them abusive e-mail messages.

Acceptable Use Policy

- Don't make personal remarks about third parties. E-mail messages can come back to haunt you.

6.2 *Defamation*

E-mails are considered to be a form of publication and the use of e-mail may constitute a libel contrary to the provisions of the Defamation Act. Both words and pictures produced in e-mails are capable of being libellous if they are untrue, ridicule a person and as a result damage that person's reputation. For these purposes, a person may include the University or another university. You must not put any defamatory statement on the University's computer system whether in e-mails or otherwise. As well as you being personally exposed to potential legal action for defamation, the University can also be exposed both for the actions of you as its employee/student and also as an online provider.

UWTSD reserves the right to remove any item that it considers may match the definition above, without notice, from any of its systems. Appropriate disciplinary action will also be considered against the individual responsible for placing such material on the UWTSD systems – see section 12, Disciplinary Measures on page 19.

6.3 *Discrimination & Harassment*

The University does not tolerate discrimination or harassment in any form whatsoever. This principle extends to any information distributed on the University's system or via the Internet. You may not put on either system any material which discriminates or encourages discrimination or harassment on racial or ethnic grounds or on grounds of gender, sexual orientation, marital status, age, ethnic origin, colour, nationality, religion or disability. Please also bear in mind the University's policy on discrimination and harassment.

Additionally, Managers should avoid bombarding the staff they supervise with e-mails containing deadlines and demands.

6.4 *Contractual Liabilities*

All Users need to be aware that they may enter into legally binding contracts with third parties via e-mail. At present the situation is that e-mails will be accepted as evidence of an intention to enter into such an arrangement, should it ever be challenged in court.

You should be certain that you intend to bind yourself or UWTSD to any arrangements you write down and send in an e-mail.

Students have no power to incur contractual liability on the part of UWTSD, and any attempt to create such a liability by a student will be dealt with most seriously.

Acceptable Use Policy

6.5 *Disclaimers*

The practice of adding a short paragraph or two intended to protect the sending institution from legal claims arising as a result of an e-mail originated from solicitors' faxes. Given the technology, they were essential in as much as the fax could be sent to the wrong number and anyone could read what arrived at the other end. Normal practice for faxes is to put the disclaimer on the first page. However, it can be argued that as e-mail can be encrypted, using a disclaimer is meaningless because "enough care" has not been taken to safeguard the contents of the message. Also, the value of any disclaimer is subject to the sender being able and willing to identify someone who misused a message, prove misuse and take the case to court.

E-mail messages are not inherently confidential. An unencrypted e-mail is the equivalent of sending a postcard, while an encrypted e-mail is analogous to sending a letter in an envelope. E-mails go over many points in Wide Area Networks and over the Internet where they can be seen by network supervisors (and hackers). A disclaimer can only create a false sense of security, when in fact you may be breaking Data Protection regulations by transmitting personal data.

Having a disclaimer does not prevent a message from being sent to the wrong person, intercepted, being read by the wrong recipient or being used against UWTSD in court. With regards to Data Protection, when transmitting personal data via e-mail, it is essential that adequate precautions are taken. The most a disclaimer can hope to achieve is to notify the recipient (or interceptor) that the contents are confidential.

For these reasons Users should not add e-mail disclaimers to their outgoing e-mails.

6.6 *Viruses in e-mail*

As you should be aware, there are many people who seem to delight in creating viruses for whatever reason. Viruses come in two main types.

The first type spread around the world automatically by infecting PCs and e-mail servers or e-mail software like Eudora, Outlook Express etc. The most famous of these, Melissa, ILoveU, Klez, are just the tip of the iceberg - at the time of writing there were over 73,000 individual computer viruses documented, many with multiple slight differences that bring the total nearer to 400,000 (see http://www.symantec.com/enterprise/security_response/index.jsp). They vary in effect from being relatively harmless to extremely destructive. The anti virus software on all PCs and servers on campus is designed to block these threats automatically, but will never be 100% effective, so please do not open attachments to e-mails that have been sent to you by someone you do not know. Just delete them - it is not worth the risk. Under no circumstances should you disable or alter the settings of the anti virus software.

With some viruses these days having become adept at avoiding removal, the only sure way (and one of the quickest) to remove a virus infection is to wipe (re-format) the hard disk of the computer and load a fresh, clean software installation onto it.

Acceptable Use Policy

The second type is spread by using psychology to get people to spread a message. These messages are not computer viruses in the true sense at all, so cannot be detected and removed by anti virus software. However, they are still harmful as they waste server resources, network bandwidth, the time of everyone who receives them and sends them on, and the time of IT Technicians. The worst sort urge you to delete files from your PC on the grounds that if you find the file the message names on your machine you have been infected by a virus. This is not true - the file named is usually a crucial system file that, if deleted, will prevent your machine from working properly in some way.

There are also the many variations on chain letters (send this to 10 people and make yourself rich), the Nigerian Money scam (come to a hotel in London, let us pay money into your account, you keep big cut) etc. etc. Even if you do not reply and instead forward the message on, it is usually a big message and hogs lots of space and bandwidth on networks.

So, to sum up,

- Delete suspect e-mails with attachments that have come from unknown sources without reading them
- Never alter the settings of the anti-virus software on your PC
- Do not forward silly messages to lots of your colleagues or friends. Just delete them.
- Never delete files on your PC just because an e-mail tells you to
- Never store files on the hard disk (the C: drive) of a lab or staff PC – Information Services may have to re-format it to remove a virus infection. Store them on a server instead.
- If in any doubt about what to do contact the Information Services Helpdesk, ITSD@tsd.ac.uk, ext. 5055

6.7 *E-mails sent to Staff that contain suspected child pornography*

The advice below relates to staff receiving in e-mails child pornography or what they consider may be child pornography. The advice is as follows:

If you receive via the University's e-mail system a pornographic image which you believe to depict a child, then:

- Immediately close the file. Do not copy it or forward it to anyone else, for any reason.
- Report the discovery to Information Services. Do not discuss the matter with anyone else.
- Information Services will conduct a preliminary investigation to attempt to identify the sender.

Acceptable Use Policy

- If the sender appears to be a student or a member of staff of the University, Information Services will report the discovery to the Pro Vice-Chancellor, who may authorise a full investigation.
- If the sender cannot be identified, Information Services will ensure that the image is deleted from all UWTSD systems.

6.8 *Out of Office Auto-replies*

Outlook (or Outlook Web Access) can be set to send an automatic reply to e-mails that your inbox receives when you are unavailable. However, such replies will go to the people who send you any SPAM that reaches your inbox, as well as e-mails from legitimate correspondents. Acknowledging this, your reply should be suitably bland.

The following is offered as a template for staff to adapt.

"I am currently unavailable. If your e-mail requires an urgent response please contact XXXXX@tsd.ac.uk or ring 01570 422351 and ask for extension XXX."

Follow this with your name and job title and don't be tempted to add anything else.

6.9 *UWTSD e-mail accounts*

As agreed by Senate, the official communications medium between the University of Wales UWTSD staff and its students is the university's own e-mail system. Therefore all students are required to have a UWTSD e-mail address (e.g. xxxx@tsd.ac.uk), and staff must use this UWTSD e-mail address to communicate with them.

In particular, staff are to discontinue the practise of harvesting the private e-mail addresses of students (e.g. student@hotmail.com) to send them e-mails, as such systems are outwith the control of UWTSD and cannot be relied upon. Staff should actively discourage their students from sending in assignments etc. using any e-mail system other than that provided by UWTSD.

Adoption of this measure will confer a considerable number of benefits on both students and staff:

- Documents such as information packs that many students need can be placed on the UWTSD web site by the webmaster and the students can be e-mailed a link to the document. This guarantees that the document students refer to is up to date as amended versions can be put on the web site quickly;
- Documents that single or small groups of students need can be sent as attachments or placed in Public Folders;
- Reduced printing costs;

Acceptable Use Policy

- Reduced stationery costs;
- Reduced manual handling costs;
- Reduced postage costs;
- Guaranteed delivery of important documents, papers, assignments etc. to and from students through systems under our control.
- Speedier communications;
- Less post to wade through;
- Less paper to file;
- Accurate and up-to-date information.

It is also better for the environment as we will not be consuming natural resources to print and move vast quantities of paper around the country.

7 Internet Use

Access to central file servers, e-mail facilities and the Internet is all accomplished by means of networking. Virtually all PCs on campus are networked together on the campus LAN and thus, by traversing JANET, to the Internet. Given this connectivity, inappropriate or offensive actions of any individual on our network reflect badly on UWTSD as an institution.

7.1 JANET AUP

As well as conforming to the UWTSD AUP, Users are also required to comply with the provisions of the JANET AUP when using the Internet. This obviously also applies to e-mails sent to off-site addresses.

The JANET Acceptable Use Policy can be found at
<http://www.ja.net/documents/publications/policy/aup.pdf>

By agreeing to the terms and conditions of this AUP you are also agreeing to abide by the JANET AUP.

7.2 Intellectual Property Rights and Copyright

Intellectual Property Rights or Copyright exists in nearly all information that can be found on the UWTSD LAN, on the Internet and in all software. Users must not perform any action which would violate any Intellectual Property Right or Copyright.

Acceptable Use Policy

7.3 *Downloading*

Users, other than technicians, may not download any software from the Internet without the express permission of the Head of Information Services.

This restriction does not apply to students in Halls downloading software for use on their own computers, as long as such downloading and use complies with all other parts of this policy.

8 **Behaviour**

8.1 *Offensive Material*

The creation, display, production or circulation of offensive material in any form or medium is forbidden.

“Offensive material” includes (without limitation)

- sex or pornography i.e. illegal material or material comparable to that available on the top shelf in a newsagent;
- terrorism;
- cults which seek to aid or abet or glorify terrorist or other illegal acts;
- controlled or illegal drugs;
- extreme or obscene material which may be likely to cause offence to another person;
- criminal skills (including software hacking);
- jokes or chain mail.

Unauthorised use of the Internet may expose both you personally and/or the University to court proceedings attracting both criminal and civil liability. You will be held responsible for any claims brought against the University for any legal action to which the University is, or might be, exposed as a result of your unauthorised use of the Internet.

Users must note that the right to academic freedom within the law and/or the necessity of downloading material from the Internet for the purposes of research do not detract from the User’s obligation to comply with the terms of this policy and in particular the obligations contained in this section on behaviour. If any User is in any doubt as to whether the investigation, viewing or downloading of material from the Internet would offend this policy and/or the general law, the User must, before attempting to access any such material, seek prior written authorisation from the Committee on Research Ethics. The procedure for seeking such permission is as follows:

- The User concerned shall write to the Registrar and Secretary, stating precisely what material is to be accessed and the academic reasons therefore.

Acceptable Use Policy

- The Registrar and Secretary shall consult the Chair of the Committee on Research Ethics, who may either make a determination or refer the request to the full Committee for a determination.
- In reaching a determination, the Chair or the Committee on Research Ethics shall consider whether the proposed use is within the general law and therefore legal and whether, if it is legal, it is desirable for the University to allow such use, having regard to such factors as: academic freedom within the law; the reputation of the University; commercial considerations.
- If the User concerned is dissatisfied with the determination of the Committee on Research Ethics or its Chair, he or she may, within seven days of receiving notification of the determination, lodge an appeal in writing with the Registrar and Secretary, stating the grounds thereof.
- The Registrar and Secretary shall refer the appeal to the Vice-Chancellor, who shall make a decision on the basis of the written evidence presented to him by the User and the reasons for the original determination by the Committee on Research Ethics or its Chair.
- The Vice-Chancellor's decision shall be conveyed to the User by the Registrar and Secretary and it shall be final.

8.2 *General behaviour*

Users must take every precaution to avoid damage to equipment caused by smoking, eating or drinking in its vicinity. In particular, smoking, eating or drinking in any student IT facilities room is forbidden.

Users must respect the rights of others and should conduct themselves in a quiet and orderly manner when using IT facilities. In particular the use of Mobile Telephones is forbidden in any student IT facilities room.

The locking of a PC in any of the student IT facilities rooms to reserve it for your personal use (by using the CTRL+ALT+DEL 'Lock Computer' option while you are logged on) effectively stops anyone else from using that computer until you return and log off properly. Users must not do this. If you need to leave the room then log off properly and take your personal belongings with you. Information Services will discipline any User found to have left a PC in any of the student IT facilities rooms locked in this way.

Users must respect published times for access to IT facilities.

Users must not invite other people into student IT facilities rooms if they are not registered students or members of staff. All pets except Guide Dogs are forbidden in student IT facilities rooms.

9 *Equipment not owned by UWTSD*

9.1 *Student PCs in Halls of Residence*

Acceptable Use Policy

Student PCs in Halls of Residence may be freely used for any purpose, as long as any use of the UWTSD campus LAN complies with this AUP and use of the Internet also complies with the JANET AUP.

Students are not allowed to:

- Set up their personal computers to act as servers, or be part of any unauthorised file sharing network like Kazaa, Napster, Grokster etc. If in doubt consult Information Services.
- Connect any device to the network socket in their room other than the computer approved for connection by Information Services
- Connect any other computing device to their one approved computer (daisy chaining) thus sharing the connection to the LAN with others.

Students must keep their accounts with UWTSD paid up or the network socket in their room may be disconnected from the LAN.

Students who have taken advantage of the facility to connect their computer to the UWTSD LAN hereby grant UWTSD Technical staff permission to inspect their computer at any time, especially if that student is suspected of breaching this AUP.

9.2 *JANET Roaming Service*

UWTSD is intending to join the JANET Roaming Service, EduRoam. This service will allow staff and students from other member institutions to log on to the network here at UWTSD using the user name and password granted to them by their home institution with no intervention needed from Information Services.

Once the service is active, and subject to the other conditions of this Acceptable Use Policy being adhered to, staff and students from other member institutions are hereby granted permission to log on to the UWTSD campus network using any of our public access PCs or using their own wireless-networking-equipped PC, free of charge.

9.3 *Other Equipment used on campus*

Anyone given temporary permission to connect their equipment to the UWTSD campus network (e.g. a conference delegate, a visiting member of staff from another HE institution etc.), may use that equipment for any purpose, as long as any use of the UWTSD campus LAN complies with this AUP and use of the Internet also complies with the JANET AUP.

Such temporary Users are not allowed to:

Acceptable Use Policy

- Set up their personal computers to act as servers, or be part of any unauthorised file sharing network like Kazaa, Napster, Grokster etc. If in doubt consult Information Services.
- Connect any device to the network socket in their room other than the computer approved for connection by Information Services
- Connect any other computing device to their one approved computer (daisy chaining) thus sharing the connection to the LAN with others.

Any fees due for the use of this facility must be paid promptly or Information Services will revoke the permission to connect to the UWTSD LAN.

Anyone who has taken advantage of the facility to connect their computer to the UWTSD LAN hereby grants UWTSD Technical staff permission to inspect their computer at any time, especially if that person is suspected of breaching this AUP.

10 Wireless Connectivity

Only Users who are authorised to do so by Information Services may attempt to connect to the UWTSD campus LAN via the Wireless Networking Access Points around campus.

11 Monitoring

Information Services keeps records in order to monitor traffic flow and system usage. These indicate the dates, times, recipients and senders of all e-mail messages. Information Services staff do not routinely inspect any of this information to check on personal use; nor do they routinely inspect the contents of any e-mail. However, in accordance with the Regulation of Investigatory Powers Act 2000, there are exceptions where some, or all of this information, including content, may be directly accessed from University systems and personal computers by authorised Information Services staff and/or external authorities.

Some examples of exceptions are as follows:

- Where a virus or large scale blanket e-mail is threatening the functionality of the whole system or is likely to delete or corrupt data;
- Where there is reasonable grounds to suspect that the University's email facilities have been misused or that university policies governing the use of e-mail have been contravened;
- At the request of the police in furtherance of a criminal investigation.

Also, if there are indications of abuse of University systems (which includes abuse of e-mail and abuse of Internet use, or where individuals may be using systems in excess of

Acceptable Use Policy

their authority) all uses of the systems may be intercepted and/or disclosed to authorised University staff and/or law enforcement officers.

The University does expect all users of its facilities to use them responsibly and in compliance with this Acceptable Use Policy.

12 Disciplinary Measures

12.1 All Users

All Users of UWTSD computing facilities are bound by the provisions of this Acceptable Use Policy.

As well as being in breach of this AUP, any User who tampers with any item of Hardware, Software or networking equipment belonging to UWTSD without permission, or who attempts to install any Software on UWTSD-owned hardware without permission is committing an offence under the Computer Misuse Act 1990. This carries a maximum penalty of 5 years in prison and/or a fine.

12.2 Penalties for Staff

In the case of staff, any detected minor breach of the Acceptable Use Policy or terms of employment as detailed in the current Staff Handbook will be dealt with informally in the first instance by the Head of Information Services.

More serious or repeated breaches will be passed to Personnel. This may lead to disciplinary action, up to and including, in appropriate circumstances, dismissal and without notice.

12.3 Penalties for Students or Visitors

In the case of Students or Visitors with access privileges, breaches of the Acceptable Use Policy will be dealt with in the first instance by the Head of Information Services. Any further breaches of the AUP within a twelve-month period will be referred to the Head of the School of Humanities and Social Sciences.

It is normal practice for Student access privileges to the network to be withdrawn while any suspected breaches of this AUP are investigated.

Penalties that the Head of Information Services can impose include indefinite withdrawal of access privileges, fines of up to £100 or both. Any costs (including staff wages) arising as a result of a student breaching this AUP will be passed on to that student in addition to any fine imposed.

Acceptable Use Policy

If the Head of Information Services decides that an appropriate punishment for an infringement of these rules would be to disconnect a student's room in halls from the campus LAN then no refund of any fee paid for this facility will be given.

If any student feels that they have been unfairly treated in respect of disciplinary measures imposed by the Head of Information Services, the student may appeal to the Pro Vice-Chancellor, who may confirm, quash or vary the penalty imposed by the Head of Information Services.

13 Absent Staff

13.1 *E-mail sent to Absent Staff*

Staff may be absent from work for a variety of reasons, including annual leave, sickness, family emergency and many others. It is important that e-mails addressed to those absent individuals are dealt with, in just the same way as any important letters would be dealt with in their absence, i.e. by someone else reading them and acting on them if necessary.

Therefore, UWTSD reserves the right to open the e-mails of any employee absent for any reason, after a suitable period of time has elapsed and after attempting to obtain the direct consent of the member of staff concerned.

Where such consent could not be obtained, and after a suitable period, the line manager of the absent employee may request that the Pro Vice-Chancellor authorise the opening of the e-mails of the absent employee.

With either the direct consent of the absent employee, or with the permission of the Pro Vice-Chancellor, Information Services can then be asked to facilitate the reading of e-mails of the absent member of staff, including overriding any passwords that may have been set.

The absent member of staff shall be informed of the decision to open their e-mails in their absence upon their return, by their line manager.

It follows that if staff are aware of an impending absence from work, they should try and arrange it so that a colleague in their department or section will deal with their e-mails for them and they have therefore given the required consent before they leave. Information Services can assist with setting up the appropriate permissions and procedures, if given enough notice.

13.2 *Files of Absent Staff*

Staff may be absent from work for a variety of reasons, including annual leave, sickness, family emergency and many others. Electronic files in the absent member of staff's U: drive, on the hard drive of their UWTSD-issued computer or on any other storage media (their File Store), including at their home or other off-campus locations, may need to be accessed in their absence for business purposes.

Acceptable Use Policy

Therefore, UWTSD reserves the right to open any File Store of an absent employee for any reason, after a suitable period of time has elapsed and after attempting to obtain the direct consent of the member of staff concerned.

Where such consent could not be obtained, and after a suitable period, the line manager of the absent employee may request that the Pro Vice-Chancellor authorise the opening of the File Store of the absent employee.

With either the direct consent of the absent employee or with the permission of the Pro Vice-Chancellor, Information Services can then be asked to facilitate the opening of the File Store of the absent member of staff, including overriding any passwords that may have been set.

The absent member of staff shall be informed of the decision to open their File Store in their absence upon their return, by their line manager.

It follows that if staff are aware of an impending absence from work, they should try and arrange it so that a colleague in their department or section can have access to any files that may be needed before they leave. Information Services can assist with setting up the appropriate permissions and procedures, if given enough notice.

14 Leavers

14.1 Staff

When Staff leave UWTSD they may have important data in their mailbox or home folders, or stored on their PC, so the line manager of the departed employee needs to tell Information Services who should receive this data, with a time limit of one month from the date the user left.

Information Services will only delete such data before the month is up with the written approval of the relevant line manager. If no instructions are received, one month after making the request Information Services technical staff will delete the data.

The same line manager also needs to tell Information Services who, if anyone, should receive any e-mails sent to the e-mail address(es) of the departing employee. E-mail forwarding of this type will be removed after three months, which should be a sufficient length of time for all regular e-mail correspondents of the departed employee to be told who they should now contact at UWTSD.

Departing staff should ensure that they make aware any of their e-mail correspondents that their xxxxx@tsd.ac.uk e-mail address can no longer be used to contact them personally, and that e-mails addressed to their old xxxxx@tsd.ac.uk e-mail address may be automatically sent to another UWTSD employee.

Acceptable Use Policy

Departing staff should also ensure that they remove any files of a personal nature from their file stores, and personal e-mails from their e-mail inbox or sub-folders, as these stores will be examined after their departure to ensure no business critical information is lost.

14.2 *Students*

When students have left UWTSD their network accounts, e-mail accounts and any files left on the network will be permanently deleted.

They should ensure that they make aware any of their e-mail correspondents that their xxxxx@tsd.ac.uk e-mail address can no longer be used.

14.3 *E-mail Forwarding*

E-mail forwarding to off-campus addresses for students or staff who have left UWTSD is not permitted under the terms of our e-mail server licence, and is against UWTSD policy.