Glyndŵr University Network & IT Facilities

Conditions of use, security policy for students & visitors.

Version: *2.0*

Issued: *07/11/2011*

Reference: *POIT071111*

Author: *Robert Stockton*

Last Reviewed: *01/07/2015*

1. **Conditions of Use**
These rules apply to students and visitors (who have been authorized) using any computer hardware or software within the University, including access to external services from Glyndŵr University, and the accessing of Glyndŵr University services using any remote access mechanism. Students are entitled to a network account on the University network. This account will include access to software supported by Glyndŵr University, access to the Internet and email facilities.

Your use of these facilities depends on you obeying the Conditions of Use, including the Security Policy. Glyndŵr University reserves the right to revoke access to its IT facilities if you do not comply with these Conditions, or if it needs to retain system integrity and security. Breach of these regulations may also lead to disciplinary action being taken and may also break criminal or civil law.

If, for legitimate academic purposes, you think you need to undertake activity that might be considered inappropriate under these guidelines, you must obtain IT Services written approval before you undertake any such activity. We may require you to supply a statement of support from your Head of School.

2. **Security Policy**
2.1. Passwords
You are responsible for the use of your account. You may be held responsible for any actions made by another person using your account, either with or without your consent.

A password for the account must be changed on a regular basis: once a month is recommended. Passwords should not be disclosed to anyone and should never be written down.

You should not write down your password in such a way that someone else might have access to it.

2.2. Software licensing
You must not install any unlicensed software onto the University's computers. We may remove without notice any such software that we find.

2.3. Access to computer systems
It is a criminal offence under the Computer Misuse Act (1990) to gain access to a computer system for which you do not have an "account" (publicly accessible computer systems such as Web servers are not included here). Similarly you must not make any unauthorized changes to programs or data. Hacking is strictly forbidden and will be treated very seriously by Glyndŵr University. This applies equally to systems on the Glyndŵr University network and external systems. Our definition of hacking includes activity that suggests that you are going to try to gain unauthorized access to systems.

The installation or storage of material or URL references referring to hacking will be considered equivalent to an attempt at hacking.

2.4. Computer virus protection
Computer viruses are programs written with malicious intent. Do not introduce or risk introducing viruses or similar malicious programs to Glyndŵr University facilities. It is your responsibility to ensure that all files which you store on local or network disks are free from viruses.

2.5. Obscenity
Glyndŵr University's IT facilities are provided for approved academic purposes only and should not be used for storing, transmitting or gaining access to inappropriate material. You must not use Glyndŵr University's IT facilities to obtain, disseminate, store or display material which is deemed to be obscene, pornographic or excessively violent. We treat the abuse of our facilities in this way very seriously and we involve the police where appropriate.

2.6. Physical security
Laptops and other highly desirable items should not be left unattended at any time due to the risk of theft or misuse. It is highly advisable to label devices and USB memory sticks with your name and contact details to aid in identifying the owner and returning misplaced items.

3. **Acceptable use of network facilities**

Access to the Internet from Glyndŵr University is provided by way of the UK's Joint Academic Network (JANET) service to which Glyndŵr University is connected. It is a condition of every JANET connection that users abide by the JANET "Acceptable Use Policy". The full Acceptable Use Policy is available on https://community.ja.net/library/acceptable-use-policy

3.1. Email and Web postings
You should not send any messages which: harass, threaten or intentionally embarrass any intended recipient; contain offensive or profane language; or contain hateful, racially or ethnically objectionable content.

Spamming and the transmission of "chain" mail are not allowed. Your messages must clearly identify the true sender - i.e., you must not send mail pretending to be from someone else.

3.2. Network traffic loads
You must not cause overloading of internal or external networks by creating sustained high network traffic loads.

3.3. Consideration for other network users
You must not alter the work of others by interfering with their data. You must not violate the privacy of other users by reading their e-mail, confidential stored documents, screen displays or printouts without their consent.

3.4. Creation of internal network services
You must not create a Server including Web, File, Printer Servers, nor any other IP service without obtaining the agreement of the IT Services Department.

4. Responsible use of resources
You are provided with networked IT facilities to help you with your academic work. This principle should guide you in your use of Glyndŵr University computer facilities. Social and recreational use of resources, where it prevents other people from making full use of the facilities for their intended purposes, is not appropriate and we may restrict or remove your access to facilities if you are doing this.

You should always leave computer equipment so that it is ready to be used by other people. You must not interfere with or disable any Glyndŵr University computer equipment in any way.

5. Compliance with legislation
Your use of computer facilities must also comply with the law. Some of the relevant legislation is contained in:

At the time of writing the relevant Acts of Parliament includes but is not limited to: Computer Misuse Act 1990, Criminal Justice and Public Order Act 1994, Copyright, Designs and Patents Act 1988, Trade Marks Act 1994, Data Protection Act 1998, Regulation of Investigatory Powers (RIP) Act 2000, Protection of Children Act 1999, Freedom of Information Act 2000, and the Telecommunications (Data Protection and Privacy) Regulations 1999, Telecommunications (lawful business practice) (interception of communications) regulations 2000. Where your conduct involves a breach of the law, you must expect us to involve the police.

6. Responsibilities of the IT Services department
We will try to provide the best and most reliable services that we can. User data on the University fileservers is regularly backed up. . We are not responsible for any losses or damage caused by failure of the systems provided.

We will respect your privacy so long as you obey the Conditions of Use. This means that we will not examine the contents of any files you may store on the network or data that your receive or transmit, unless we have reason to suspect a breach of the Conditions of Use. We may, however, scan user directories and monitor traffic logs and user account activity. If we find evidence of possible misuse of facilities we may investigate and this may involve examination of the contents of files. We may suspend your access to your account while we do this. We will not withdraw your access to the service without good reason.

For a first minor breach of these Conditions, we will probably suspend your account for a period and you will be required to see the Head of IT Services and undertake not to repeat the offence before your access is reinstated. Further breaches will be treated much more seriously.

More serious breaches of Conditions of Use will result in disciplinary proceedings. In the most serious cases, and where the law has been broken, we will involve the police.