



Rules Governing Student Behavior
(PNG UNIVERSITY OF TECHNOLOGY ACT 1986)
Laws Breached as a Consequence of Defaulting Computer Labs Rules

Computer Laboratory - RULES 2016

1. Students should not remove equipment (including cables, or components of ICT equipment) belonging to the University from computer classrooms.
2. Students should not intentionally damage or disable ICT equipment in computer labs. This includes damage to the cables, mice, disk drives or any hardware components.
3. Students should not login to other student's areas, or staff areas, on the file server unless they have written permission to do so.
4. Students should not destroy files that do not belong to them, i.e. Students may only delete files that are stored on their "home" area on the server.
5. Students should not change parts of the computer hardware/software system which will disable it, or change its performance in any way that will affect other users.
6. Students should not leave unattended computers that they are logged in to the server. Any student or staff member has the right to reset a computer which is logged on the server but is unattended, even if the user has left an explanation.
7. Students should not store any material that could be considered pornographic, or any other textual or graphical that breaks PNG law, on the file server or other storage media.
8. Students should not play games on classroom computers.
9. Students should respect and honor any instructions or directions issued by classroom monitors (with ID) that are officially nominated by a department.
10. Students should obey all requests by the classroom monitors who supervise the computer classroom in the evenings and on the weekends.
11. Students should not consume food beverages or buai in the computer classrooms, nor will they smoke.
12. Students are expected to report breaches of security, theft of equipment, suspicious events, and to challenge anybody who they consider might not be part of the University.

Subject to the provisions relating to penalties in the existing Computer Laboratory Rules and UNITECH Computer Network Rules, any student found to have breached these RULES relating student misconduct, stealing, destroying, removing, sabotage or disobeying shall be guilty of an offence.

Penalties

- (a) For first offence, student is locked out from accessing the network for 7days.
- (b) For second offence, student is locked out from accessing the network for 14 days and referred to the disciplinary committee.
- (c) For third offence, student is locked out from accessing network, is referred to the disciplinary committee and faces expulsion from studies.

NOTE:

I have read and understood the rules and hereby declare that I abide by these rules.

NAME:

ID #:

DEPARTMENT:

COURSE/YEAR

SIGNATURE:

DATE:

DEPT. WITNESS & SIGN:

DATE:

Logon and Logout of the Student computer system

You can log into the student computer system by going to one of Students computer laboratories around the campus. The procedure to login is given below.

Login using Windows XP & Windows 7:

1. Turn on the computer and monitor. Windows will take a moment to load simultaneously.
2. When a dialogue box appear press the three keys, CTRL+ALT+DEL.
3. The next dialogue box will appear prompting you to enter your USERNAME, PASSWORD and DOMAIN.
Eg. USERNAME: 00400231abcd
PASSWORD: drow7Ssap
DOMAIN: STUDENT
4. The next dialogue box will prompt you to change your password.
5. Please enter a eight or more character password. CAUTION; Do not reveal your password to anyone. Individuals must keep id/password secure.
6. Click OK to continue.

To log out,

1. Click on the Start bar and Select **Shutdown** or **Logoff**.
2. A dialogue box appears for you to select various options.
3. Select SHUTDOWN/Log off 00400231 computers..
4. Click Ok.

Email – Google Accounts

Starting this year (2016), UNITECH will host student email service on Google. You may access emails from all student computers.

To use the email, follow the steps:

1. Start Internet Explorer, Mozilla Firefox or Google Chrome
2. Enter following text in address bar
<https://accounts.google.com/ServiceLogin>
3. Enter your email ID and password as provided on your ID slip.

Home Area

When your account on the student domain system is created, you are allocated 50 megabytes of disk space for your use. This space, accessible from any computer on the system, is known as your home directory (area). Each time you log in to the system, using your user ID (login ID) and your password, you authenticate to the system that you are in fact who you say you are. Once the system has authenticated your login, you can make changes, such as creating new files and editing existing files in your home directory.

ICT S Helpdesk

The ITS Help Desk is your first point of contact for your technology needs. The staff, a mixture of full-time and part-time personal, all have training in technical and customer service skills. In addition, the Help Desk consultant, when necessary, will put you in touch with ICTS's many advanced technology professionals.

When contacting the Help Desk it is important to have relevant information handy; such as your computer make and model, software version, any error messages you've received and the steps you've taken so far. This will allow the consultants to have a better understanding of your issue and will take the first step towards resolution.

You can contact ICTS Help Desk via e-mail, helpdesk@its.unitech.ac.pg or via phone on 473-4212 (office hours only) or visit our office at Haus Europa.

Student account

All current undergraduate and graduate students are automatically provided with an account on the Student computer system. A user ID and initial password are given to each student at the beginning of the school year.

Prohibitions

The following activities are strictly prohibited.

1. To use another person's user ID.
2. To access prohibited sites.
Porn, violence, drug, warez, gambling,
3. To download following contents.
Music file (e.g. mp3, wma, ogg etc.)
Video file (e.g. avi, mov, flv etc.)
Game
Or any contents that the UNIVERSITY regard as undesirable.
4. To use P2P software.
5. To hack another person's system.
6. To attach prohibited contents on email.
7. To slander other person(s)/organization(s).
8. To download above prohibited contents onto the students' server is not allowed. If those kind of files are found, those files will be removed without notice.