Table of Contents

INTRODUCTION ........................................................................................................... 4
ICT ACCEPTABLE USE POLICY .................................................................................. 4
AIMS AND OBJECTIVES ............................................................................................. 4
THE CNS SERVICE DESK ......................................................................................... 4
SECTION A – STUDENTS INFORMATION .................................................................. 5
SECTION A1 - OPEN ACCESS COMPUTER LABORATORIES (LABS) ....................... 5
SECTION A2 - RULES OF THE LAB ......................................................................... 6
SECTION A3 - OFFICE OF RESIDENCE LIFE COMPUTER (LABS) ......................... 6
SECTION A4 - GETTING STARTED USING COMPUTING FACILITIES .................... 6
SECTION A5 - PASSWORD RESET ............................................................................. 6
SECTION A6 - HOW TO REGISTER FOR PASSWORD SELF SERVICE .................... 7
SECTION A7 - ACCESS TO THE NETWORK DRIVE (H: DRIVE) ......................... 8
SECTION A8 - CONFIGURATION SUPPORT ............................................................... 9
SECTION A9 - PRINTING & SCANNING .................................................................... 9
SECTION A9.1 – PRINTING ..................................................................................... 10
SECTION A9.2 SCAN TO EMAIL FUNCTION .............................................................. 14
SECTION A9.3 COPY FUNCTION .............................................................................. 18
SECTION 10 - EMAIL – GENERAL .......................................................................... 21
SECTION 10.1 - OUTLOOK 2010 EMAIL SETUP .................................................... 22
SECTION B - STAFF AND STUDENTS (INFORMATION AND CONFIGURATION –WIRELESS AND VPN) ................................................................. 28
SECTION B1 - EMAIL – SPAM ................................................................................ 28
SECTION B2 - WHAT IS SPOOFING? ................................................................. 28
SECTION B2.1 - HERE IS HOW SPOOFING OCCURS: ......................................... 28
SECTION B2.2 - WHAT IS ABUSE@WITS.AC.ZA - AND HOW TO USE IT ............. 29
SECTION B3 - HARDWARE AND DEVICES ............................................................ 29
SECTION B4 - SETTING UP YOUR MAIL ............................................................. 30
SECTION B4.1 - IPHONE EMAIL SETUP ............................................................... 30
SECTION B4.2 - ANDROID EMAIL SETUP ............................................................. 31
SECTION B5 - ANTIVIRUS ..................................................................................... 33
SECTION B6 - VIRTUAL PRIVATE NETWORK (VPN) ............................................. 34
SECTION B6.1 - WINDOWS 7 & 8 CHECKPOINT VPN ........................................ 35
SECTION B6.2 - WINDOWS 8 CHECKPOINT VPN .............................................. 38
SECTION B6.3 - VPN FOR APPLE MAC ............................................................... 40
SECTION B6.4 - VPN ON UBUNTU ...................................................................... 44
SECTION B7 - PROXY SETTINGS .......................................................................... 59
SECTION B7.1 - PROXY SETTINGS ON WINDOWS INTERNET EXPLORER ......... 59
SECTION B7.2 - PROXY SETTINGS FOR FIREFOX/MOZILLA .............................. 60
SECTION B7.3 - PROXY SETTINGS ON APPLE MAC OS X VERSION 10.3.X ......... 63
SECTION B7.4 - PROXY SETTINGS ON APPLE MAC FOR FIREFOX/MOZILLA .. 67
SECTION B8 - WIRELESS ACCESS FOR LAPTOPS AND NOTEBOOKS ............... 70
SECTION B8.1 - WIRELESS SETUP FOR WINDOWS 8 ....................................... 70
SECTION B8.2 - WIRELESS SETUP FOR WINDOWS 7 ....................................... 77
SECTION B8.3 - INTERNET EXPLORER OR GOOGLE CHROME USERS .......... 81
SECTION B8.4 - WIRELESS SETUP FOR MOZILLA FIREFOX USERS ................. 82
SECTION B8.5 - WIRELESS ACCESS FOR APPLE MAC AIRPORT, ................. 83
SECTION B8.6 - SAFARI ...................................................................................... 84
SECTION A7 - WIRELESS ACCESS FOR LINUX(UBUNTU) .............................................................. 89
SECTION B9 - WITS MOBILITY – SMARTPHONES ETC............................................................ 93
SECTION B – 9.1 CONFIGURING YOUR DEVICE ON THE WITS WI-FI NETWORK .................. 93
SECTION B – 9.2 REGISTER/DELETE A MOBILE DEVICE VIA A WEB BROWSER ... 96
SECTION B10 - EDUROAM® SERVICE ................................................................................... 100
SECTION B11 - ENHANCED IT SERVICES FOR POSTGRADUATE STUDENTS ................. 102
SECTION B12 - FLEXIBLE INTERNET OPTIONS ................................................................. 102
SECTION B13 - PRINTING SUBSIDY ....................................................................................... 102
SECTION B14 - COLLABORATION AREAS ............................................................................ 102
SECTION B15 - ELEARNING ................................................................................................. 102
SECTION C - STAFF ICT SECTION ......................................................................................... 104
SECTION C1 - NEW USER CONFIGURATION .......................................................................... 104
SECTION C2 - PASSWORD RESET .......................................................................................... 104
SECTION C3 - EMAIL SERVICES ............................................................................................ 108
SECTION C3.1 - EMAIL DISTRIBUTION LIST ....................................................................... 108
SECTION C3.2 - MODIFYING AND MANAGING (ADDING/REMOVING) MEMBERS TO THE LIST ............................................................................................................. 109
SECTION C3.3 - SETTING UP A SHARED MAILBOX ............................................................... 112
SECTION C3.4 - ADD A SHARED MAILBOX ON A SEPARATE OUTLOOK PROFILE .................. 112
SECTION C3.5 - HOW TO ADD A SHARED/DEPARTMENTAL MAILBOX IN OUTLOOK 2016 ON AN APPLE MAC .............................................................................................................. 115
SECTION C3.6 - HOW TO SEND A MAIL ON BEHALF OF A DEPARTMENTAL MAILBOX. (SAME PROFILE) ................................................................................................................................. 118
SECTION C3.7 - HOW TO ACCESS A DEPARTMENTAL MAILBOX VIA WEBMAIL ............... 119
SECTION C3.8 - HOW TO GIVE ANOTHER USER VIEW PERMISSIONS ON A DEPARTMENTAL MAILBOX ................................................................................................................................. 121
SECTION C3.9 - SHARING CALENDERS AND GRANTING ACCESS .......................................... 123
SECTION C3.10 - EMAIL SOFTWARE ..................................................................................... 123
SECTION C3.11 - EMAIL MAILBOX SIZE INCREASE .............................................................. 123
SECTION C4 - ORACLE EMPLOYEE SELF SERVICE ............................................................... 124
SECTION C4.1 - CHANGING YOUR OFFICE TELEPHONE NUMBER AND UPDATING INFORMATION ON I-WITS .............................................................. 125
SECTION C4.2 - SETTING YOUR PREFERRED NAME (EMAIL) ............................................. 126
SECTION C4.3 - E-SERVICES - NEW WEB SITE .................................................................... 128
SECTION C4.3.1 - FAXEMAIL ............................................................................................... 129
SECTION C5 - HARDWARE AND DEVICES ............................................................................ 129
SECTION C5.1 - HARDWARE PURCHASING / PROCUREMENT ............................................... 129
SECTION C5.2 - FAULTY HARDWARE ..................................................................................... 130
SECTION C5.3 - SECURING DESKTOP PCS ......................................................................... 130

Please note this guide is a reflection of student ICT services at the time of going to print. As a result of ongoing improvements and enhancements to the student ICT infrastructure, some parts of this brochure may become outdated during the course of the academic year. If in doubt, please contact CNS Service Desk on the 1st floor, South West side, Senate House or contact itstudenthelp@wits.ac.za or 011- 717-1717

Version 8.0.1 2016
INTRODUCTION

CNS (Computer & Network Services) provides a range of IT related services to the University community across Wits campuses. A CNS Service Desk Student Assistant is also on hand at each of the Open Access CNS Managed Computer Laboratories to help the students with computer related questions. (Service Desk Student Assistant available Mon-Fri between 08h00-17h00).

ICT ACCEPTABLE USE POLICY

All users must abide by the Acceptable Use Policy when making use of any Wits University Computer Facilities. A copy of the policy is on website address:


AIMS AND OBJECTIVES

The aim of this guide is to provide information about services offered by CNS to the University Community to make the most effective and efficient use of the computer facilities and services available for consumption. You would be advised to attempt to follow the instructions provided in this guide before requesting assistance.

NB. Personal devices need to adhere and meet the standard requirements of the University.

THE CNS SERVICE DESK

The Service Desk is the central point of contact between the university community and Computer & Network Services. Call the Service Desk if you have IT related issues, problems with logging on, accessing your e-mail box or using Internet or standard software programs.

The CNS Service Desk offers configuration support to the University Community for personal devices i.e. setting up to access email and Internet. As a user of the Wits University network you are required to ensure that your computer is adequately protected with antivirus software. You are also responsible for ensuring the adequate backing up of your own data prior to CNS providing you with configuration support.

CONTACT DETAILS

CNS Service Desk
1st Floor, West Wing, Senate House Building, East Campus Tel: 011 717 1717
E- mail: ithelp@wits.ac.za or itstudenthelp@wits.ac.za
SECTION A – STUDENTS INFORMATION

SECTION A1 - OPEN ACCESS COMPUTER LABORATORIES (LABS)

NB. All CNS Open Access Undergraduate (UG) Computer Labs are available to students as well as staff

Abbreviations Used:

- CNS: Computer & Network Services
- WEC: WITS Education Campus
- UG: Undergraduate
- EC: East Campus
- PG: Postgraduate
- WC: West Campus
- SH: Senate House
- MS: Medical School Campus

CNS Open Access Labs

<table>
<thead>
<tr>
<th>CNS Open Access Labs</th>
<th>Location</th>
<th>Number of PCs</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAST CAMPUS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CNS PG LAB - SH1029</td>
<td>1st floor, West Wing, Senate House SH1029</td>
<td>21</td>
</tr>
<tr>
<td>CNS UG LAB - SH1101</td>
<td>1st floor West Wing, Senate House SH1101</td>
<td>44</td>
</tr>
<tr>
<td>CNS UG LAB - SH1099</td>
<td>1st floor West Wing, Senate House SH1099</td>
<td>15</td>
</tr>
<tr>
<td>CNS UG LAB - HP ZONE</td>
<td>1st floor West Wing, Senate House, Mezzanine</td>
<td>44</td>
</tr>
<tr>
<td>WEST CAMPUS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CNS UG LAB - FNB2A (AUD)</td>
<td>First National Bank Building (FNB) Ground Floor, Auditorium</td>
<td>53</td>
</tr>
<tr>
<td>CNS PG LAB - FNB2A1 (MEZ)</td>
<td>First National Bank Building (FNB) 1st floor, Mezzanine</td>
<td>27</td>
</tr>
<tr>
<td>CNS UG LAB - FNB 2B</td>
<td>First National Bank Building (FNB) Ground floor</td>
<td>69</td>
</tr>
<tr>
<td>CNS UG LAB - FNB 105</td>
<td>First National Bank Building (FNB) 1st floor, South</td>
<td>97</td>
</tr>
<tr>
<td>CNS UG LAB - CLM1</td>
<td>Commerce, Law &amp; Management (CLM) Library, 1st Floor</td>
<td>138</td>
</tr>
<tr>
<td>WITS EDUCATION CAMPUS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CNS UG LAB - WEC-01</td>
<td>Boyce Block, Ground Floor, BL36</td>
<td>29</td>
</tr>
<tr>
<td>CNS UG LAB - GLASS LAB01</td>
<td>Marang Block, Ground Floor</td>
<td>96</td>
</tr>
<tr>
<td>CNS PG LAB – WEC PG-01</td>
<td>Botshabeleng Block, First Floor, B105</td>
<td>28</td>
</tr>
<tr>
<td>CNS L247 Lab – 50</td>
<td>Leseding block</td>
<td>50</td>
</tr>
<tr>
<td>CNS L249 Lab – 30</td>
<td>Leseding block</td>
<td>30</td>
</tr>
<tr>
<td>CNS L250 Lab – 34</td>
<td>Leseding block</td>
<td>36</td>
</tr>
<tr>
<td>CNS L251 Lab – 52</td>
<td>Leseding block</td>
<td>52</td>
</tr>
<tr>
<td>CNS L253 Lab – 30</td>
<td>Leseding block</td>
<td>36</td>
</tr>
<tr>
<td>Medical School Campus</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CNS UG LAB - MS-01A</td>
<td>Medical School, 3rd Floor</td>
<td>26</td>
</tr>
<tr>
<td>CNS UG LAB - MS-01B</td>
<td>Medical School, 3rd Floor</td>
<td>33</td>
</tr>
</tbody>
</table>

The Internal PC speaker has been disabled in all CNS Open Access LAB machines. You are encouraged to use headphones when accessing the online audio content of a virtual training course.

You may not unplug any computer from the network or use the computer charge point for your laptop device. There are provisioned areas specifically for the purpose. The seat in the lab is dedicated for the student who does not have access to his/her own computer device.
SECTION A2 - RULES OF THE LAB

In order for all users to equally enjoy these facilities, please observe these rules of conduct:

- No Food
- No Drinks
- No Eating or Drinking in the Lab
- No Sleeping in the Lab
- No Unauthorized or Unaffiliated Visitors
- No Games of Gaming
- Say NO to internet piracy
- No Smoking
- SILENCE PLEASE

SECTION A3 - OFFICE OF RESIDENCE LIFE COMPUTER (LABS)

NB. The following computer laboratories are for the exclusive use of students living at the respective University Residences:

<table>
<thead>
<tr>
<th>Residence Laboratory Name</th>
<th>Location</th>
<th>Number of PCs</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAST CAMPUS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jubilee Hall</td>
<td>East Campus</td>
<td>8</td>
</tr>
<tr>
<td>Men's Residence</td>
<td>East Campus</td>
<td>13</td>
</tr>
<tr>
<td>Sunnyside Residence</td>
<td>East Campus</td>
<td>10</td>
</tr>
<tr>
<td>WEST CAMPUS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bemato</td>
<td>West Campus, Bemato Residence</td>
<td>10</td>
</tr>
<tr>
<td>David Webster</td>
<td>West Campus, David Webster Residence</td>
<td>6</td>
</tr>
<tr>
<td>West Campus Village</td>
<td>West Campus, West Campus Village Residence</td>
<td>4</td>
</tr>
<tr>
<td>OTHER RESIDENCE LOCATIONS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Braamfontein Centre</td>
<td>23 Jorissen St, Braamfontein</td>
<td>10</td>
</tr>
<tr>
<td>Esselen Street Residence</td>
<td>7 Esselen St, Hillbrow</td>
<td>12</td>
</tr>
<tr>
<td>Parktown1</td>
<td>3 Blackwood Rd, Parktown</td>
<td>7</td>
</tr>
<tr>
<td>Parktown2</td>
<td>20 Rockridge Rd, Parktown</td>
<td>10</td>
</tr>
<tr>
<td>SOR (Ernest Oppenheimer)</td>
<td>5 Tremonton Plc, Parktown</td>
<td>10</td>
</tr>
<tr>
<td>Knockando</td>
<td>21 Rockridge Rd, Parktown</td>
<td>11</td>
</tr>
<tr>
<td>Campus Lodge</td>
<td>48 De Korte Street Braamfontein (Non Networked)</td>
<td>Network points for laptops</td>
</tr>
<tr>
<td>Graduate Lodge</td>
<td>34 Jorissen Street, Braamfontein (Non Networked)</td>
<td>2</td>
</tr>
</tbody>
</table>
SECTION A4 - GETTING STARTED USING COMPUTING FACILITIES

The student portal is your single point of entry for your Wits E-Resources such as email, calendaring, eLearning etc. Further information is available on the portal web site.

URL (Web Address): http://my.wits.ac.za

The creation of all student accounts (returning and new) is an automated student process as part of your registration. To get the best use out of this please note the following pointers.

Username: Your student number
Password: Your password is sms’d to you during registration on the cell number recorded from the completed registration form.

If using a passport number that contain letters as well as numbers, ensure you enter the letters in UPPERCASE. If you have changed your cell number in the interim, please visit Student Enrolment Centre to have your information update or alternatively use the Student Self Service to update your details.

SECTION A5 - PASSWORD RESET

Passwords can be reset via Password Self Service which you can do on the Student Portal home page where you would be required to register as displayed on the next page.

In order to make use of this service you have to register on the Password Self Service web site whilst you are still using a valid password.
SECTION A6 - HOW TO REGISTER FOR PASSWORD SELF SERVICE

Online Password Reset Service

Go to https://my.wits.ac.za/ and under Password Self Service click “reset it”.

Enter STUDENTS\Student number and then click Next.

Enter your ID/Passport and Wits Number (ICAM number with the first two digits replaced by letter “W” and leave out the last two digits), then click Next.
Enter a new password** and confirm it, then click Next.
** Password must be minimum 9 characters’ long
** Password must be Alphanumeric (Letters and numbers)
** Password cannot be any of the previous 10 student passwords

Your student password has been successfully reset. You can now log into student email, CLE/SAKAI and Wits network.

**** Password will expire every 600 days
*****If you log on to a PC added to the student domain, you will receive a reminder to change your password 20 days before it expires.

N8. The next time you log on, remember to use the NEW password.

SECTION A7 - ACCESS TO THE NETWORK DRIVE (H:\ DRIVE)

As a student user in a CNS Open Access LAB you will have a network drive available to you to store your academic documents electronically. This network drive is labelled as the H:\ drive in your Windows Explorer.

You have a limit of 50MB of network space available to you, use with care.
SECTION A8 - CONFIGURATION SUPPORT

Configuration Support which involves and offers basic assistance to users (staff and students) who own non-Wits hardware in terms of the following:

1. Configuring the Local Area Network Interface for use on the Wits Network
2. Configuring the Wireless Network Interface for use on the Wits Network
3. Installation and basic configuration of VPN (Virtual Private Network) software
4. Configuration of Internet Proxy settings and email setup

It is important to point out that the service does not include support of Operating System updates/patches, data backups, antivirus support, trouble-shooting of any of the above mentioned services, etc. Should a user require more than Configuration Support, the Service Desk will assist in providing contact details of University approved vendors who would provide such support. The service is purely aimed at helping those users with working, up-to-date computers to connect successfully to the Wits network. Users of this service will be guided by the CNS Service Desk to complete an Authorisation & Indemnification form prior to Configuration Support commencing.

This is a walk-in service and as such, users would need to bring their PCs, laptops, or other mobile devices to the CNS Service Desk for Configuration Support to the 1st floor, Senate House (West Wing), East Campus.

SECTION A9 - PRINTING & SCANNING

Printing is available to you in the CNS Open Access LABS and University Libraries at a cost:

<table>
<thead>
<tr>
<th>DESCRIPTION</th>
<th>Cost Per Page (incl VAT and paper)</th>
</tr>
</thead>
<tbody>
<tr>
<td>A4 SINGLE SIDED (SIMPLEX) - BLACK &amp; WHITE</td>
<td>R0.39</td>
</tr>
<tr>
<td>A4 DOUBLE SIDED (DUPLEX) - BLACK &amp; WHITE</td>
<td>R0.55</td>
</tr>
<tr>
<td>A4 SINGLE SIDED (SIMPLEX) - COLOUR</td>
<td>R2.88</td>
</tr>
<tr>
<td>A4 DOUBLE SIDED (DUPLEX) - COLOUR</td>
<td>R5.69</td>
</tr>
</tbody>
</table>

Follow the process below to print to a printer in a CNS Open Access Lab.

You would need to first ensure that you have enough money available on your ICAM Access Card in order to proceed with printing as this is NOT shown on the print client software before a print job that is sent through.

Please contact ICAM on 011 717 1830 if you are unsure of how to load money on your ICAM Access Card, or if you do not know where the kiosks are to load money onto your access card or to check your balances.
SECTION A9.1 – PRINTING

Open document which you would like to print
Select File
Select print

Select a Student-Color or Student-BW print driver
Select “Print”

Swipe your ICAM Card on the right hand side of the Equitrac Terminal
Select: Print (F1)

If your Kudu Bucks Balance has insufficient CREDIT, you will not be able to Print.
PLEASE ADD MORE FUNDS TO YOUR KUDU BUCKS ACCOUNT AND CONTINUE PRINTING

STEP 5: Select your Print Job using the up and down arrows

You have the following Options:
Print the selected document (F1)
Delete the selected print job (F2)
End the Print session (F3)
The Device begins printing

Select End to complete the Session
SECTION A9.2 SCAN TO EMAIL FUNCTION

Select Fax / Scan

Select: Address Search, then Search

OR
Type in your Student Number utilising the keyboard on the panel, and select Start Search

OR
Select your Email address and select OK

OR
STEP 5: Hit the Start Button to commence scanning

OR

OR
SECTION A9.3 COPY FUNCTION

Swipe your ICAM Card on the right hand side of the Equitrac Terminal

Select: Copy [F2]
If your Kudu Bucks Balance has insufficient CREDIT, you will not be able to Copy.

Please add more funds to your Kudu Bucks account and continue copying.

Complete your copy requirements.

OR
Select End to complete the Session

NB: REMEMBER TO LOGOUT TO PREVENT OTHERS FROM USING YOUR ACCOUNT!

NB: Print Jobs are only stored for 72 Hours.
SECTION 10 - EMAIL – GENERAL

EMAIL SERVICE

Postgraduate research students are automatically granted the following email service:

The undergraduate student receives an unlimited quota on Google Mail. This increased quota will allow the research student to accumulate and manage substantial correspondence with their research colleagues.

Postgraduate research students can also obtain a staff like email address which enhances the standing of the research student as a representative of the Faculty that is supporting the research.

NB. This email address will be subject to approval from the relevant Faculty.

On registration all students will be allocated an Active Directory (AD) account and granted access to the WITS network and the Internet from the CNS Open Access Computer Laboratories.

You also receive a WITS email account and you can use either one of the following email addresses that has been allocated to you:

- StudentNumber@students.wits.ac.za
- FirstName.Surname@students.wits.ac.za

Access to your Wits email will only be available through the student portal (http://my.wits.ac.za) or directly via Google Mail.

Your email account size is unlimited as per Google Mail System.
All electronic University correspondence will be sent to your Wits email address. If you are using another email address follow the instructions below to forward the emails sent to you by the University.

**SECTION A10.1 - OUTLOOK 2010 EMAIL SETUP**

Click on the Start Button, then go to Control Panel.

In Control Panel, click on Mail.

Click on Show Profiles.
Click on the **Add**

Choose a meaningful name of your choice as the **Profile Name**, then click **OK**

The next screen will resemble the one below. Select **Manually configure server settings or additional server types** and then click on **Next**.
Select **Internet E-mail** and click **Next**

Configure your profile as seen in the screen shot below. i.e:

- **Your Name**: Your Name & Surname
- **E-mail Address**: Studentnumber@students.wits.ac.za
- **Account Type**: IMAP
- **Incoming mail server**: imap.gmail.com
- **Outgoing mail server**: smtp.gmail.com
- **Username**: Studentnumber@students.wits.ac.za
- **Password**: Your Password

Make sure that the **Require logon using Secure Password Authentication (SPA)** option is checked and then click on **More Settings**

Under the **Outgoing Server** tab. Check both the **My outgoing server (SMTP) requires authentication** as well as the **use same settings as my incoming mail server** options
Under the **Advanced** tab, for the **Incoming server** choose SSL from the drop down list and use port 993. For the **Outgoing Server** select SSL from the drop down list and then use port 465. Then click on the **OK**.

![Email Settings Screenshot]

After clicking on the next button, the two tasks as shown in the screen shot below will then execute and must yield "**Completed**" status. Once that is done, click on the **Close**.

![Close Screenshot]

Click on **Finish**.
Go to E-mail Accounts

Make sure the account you just created is highlighted and then click on Change...

Click on More Settings …

Under the Sent Items tab, select the Do Not save copies of sent items option and then click on OK. (When using an IMAP email account, Google already sends a copy of every sent email to the sent items, so if this option is not selected, you will receive 2 copies of every sent message in your sent items folder.) Note: This option will only be available if the account has already been created as per the above process, or else it will just be greyed out.
Once again click on Next.

the two tasks as shown in the screen shot below will once again execute and show “Completed” status. Once that is done, click on the Close

It might take some time for your email to complete the initial sync, depending on your network speed and how much mail you have in your Wits student mailbox.
SECTION B - STAFF AND STUDENTS (INFORMATION AND CONFIGURATION – WIRELESS AND VPN)

SECTION B1 - EMAIL – SPAM

CNS’s email gateway blocks tens of thousands of spam email on a daily basis. Some emails cannot be confirmed as spam and therefore are allowed to be delivered to your mailbox.

WHAT IS SPAM?

The internet definition of SPAM is: - “irrelevant or unsolicited messages sent over the Internet, typically to large numbers of users, for the purposes of advertising, phishing, spreading malware, etc.”

WHAT TO DO WITH SPAM

Spam mail that arrives into the users’ email box may or may not have the words SPAM: tagged onto the subject line of the email. Most spam mails will be diverted to your Junk mail folder.

NB. MAILS CONFRIMMED AS SPAM SHOULD BE DELETED IMMEDIATELY!

Do not respond to the spam email or visit a web site link that claims you can be unsubscribed. These are often decoys used to determine whether your address is valid. If you acknowledge to a spammer that your account is active, the address becomes much more valuable and may be resold to other spammers. Spammers often falsely claim that you have requested to be on their list. Responding to such claims confirms the validity of your e-mail and makes it likely you will receive even more unwanted e-mail. Legitimate businesses will recognize and honor list removal requests, but it’s not always easy to determine whether a business has such integrity.

Should you click on ‘unsubscribe’ when you get a spam email?

No. Clicking an unsubscribe link may confirm to the spammer that your e-mail address is working and is being used actively. Such ‘live’ e-mail addresses are valuable and can be resold to other spammers, resulting in even more spam sent to you.

SECTION B2 - WHAT IS SPOOFING?

Email spoofing is forging an email header to make it look like it came from somewhere or someone other than the actual source. It is often an attempt to trick the recipient into making a damaging statement or releasing sensitive information, such as passwords.

If you’re receiving bounced (returned) emails for messages that you never sent and that use as the return address your domain and addresses you never created, then this could be a case of spoofing.

SECTION B2.1 - HERE IS HOW SPOOFING OCCURS:

A spammer finds an email address or a valid domain. (Spammers spend their days looking for these.) The spammer sends a large email campaign with this domain in the “From” address, using various email tools that prohibit easy tracing of the origin. These tools cloak, scramble or remove the header entirely. Most people assume an email came from the address it was sent from, just as they do with the return address on snail mail they receive. An innocent domain owner gets flooded with bounce messages from the email addresses that weren’t valid or have blocking capabilities. Within a week, the spammer gets shut down by his/her ISP due to excessive bandwidth, complaints from people who figured out who...
actually sent the email, etc. The spammer moves onto another domain.

Unfortunately spoofing is incredibly hard to trace, and the general suggestion to deal with it is to ignore the problem.

Spoofing is possibly the most frustrating abuse issue to deal with, simply because it cannot be stopped. Spoofing is similar to hand-writing many letters, and signing someone else’s name to it. You can imagine how difficult that would be to trace.

SECTION B2.2 - WHAT IS ABUSE@WITS.AC.ZA - AND HOW TO USE IT

Certain email addresses are reserved for a specific use. Their primary function is to make it easy for the administrators of various servers when they need to contact the most responsible person for a particular service.

The abuse@wits.ac.za address is an address where phishing mails can be reported.

DO send any phishing emails to the abuse@wits.ac.za address
DO send mails that are abusive or defamatory to abuse@wits.ac.za address
DO NOT send spam mails to the abuse@wits.ac.za address. Spam mails usually arrive from spoofed addresses and these are usually difficult to block.

SECTION B3 - HARDWARE AND DEVICES

Staff and Students who would want to purchase a desktop, laptop or device for personal use, PURCO on behalf of the South African Universities, negotiated prices with specific suppliers for specific laptops that are now being offered to qualifying staff and students.

Note: All transactions relating to the procurement of the laptops are between the computer supplier and the end-user. There is no financial gain for the University. PURCO is the Purchasing Consortium of Southern Africa

Click on http://www.stp.ac.za/
Or call 0800 22 37 33 /0800 ACERED
SECTION B4 - SETTING UP YOUR MAIL

SECTION B4.1 - IPHONE EMAIL SETUP

Go To “Settings” Add Account “Mail, Contacts, Calendars”

Select “Microsoft Exchange”

Enter the information as shown in the dialogue box above
Domain User name: Student No
Password: Email Password
Exchange Server: Studentmail.wits.ac.za

You can then choose to switch on the items you need to have on your IPhone

Your Keyboard will appear allowing you to type in the information required

SECTION B4.2 - ANDROID EMAIL SETUP

e.g. Samsung Galaxy, Samsung Galaxy SII, HTC Desire etc.

Go to “Settings”
Select “Accounts and sync”

Select “Add Account”
Select "Microsoft Exchange" Enter the information As indicated below

Please follow the above images and input credentials according to student or staff status as below:

Domain User name: **Student No**
Password: **Email Password**
Exchange Server: **Studentmail.wits.ac.za**

Domain User name: **DS\Staff No**
Password: **Email Password**
Exchange Server: **Email.wits.ac.za**

Then select **Next**

Select Default Account and Signature, Slide down to select further options if required
SECTION B5 - ANTIVIRUS

Procedure for checking for viruses on Memory Sicks (Flash Drives)

You can insert your memory flash drive/memory stick onto the pc in the lab. Eset Nod is loaded on the PC, and is visible on the bottom right hand corner of your pc. You then need to click on Eset Nod, click on Computer Scan, and select the drive you wish to scan. It will be on the list of drives. You would only need to tick the box and scan.

Alternatively, you could seek outside assistance or reformat the USB.

Formatting your memory stick will result in the loss of all information on the memory stick. Consider carefully before formatting your memory stick.

For personal devices that are not University Assets; you can connect to the one of the popular vendors below and download an antivirus application. Some of the products are free for private use and some are not. Please check the license for the product you choose.

AVG: http://www.grisoft.com/
F-Secure: http://www.f-secure.com/
Symantec: http://www.symantec.com/
ESET: http://www.eset.com/
NAI: http://www.mcafee.com/

Please note that this list is not a complete list of anti-virus vendors, and the Eset product is available at University negotiated rates from CNS. Contact the Service Desk for contact information.
SECTION B6 - VIRTUAL PRIVATE NETWORK (VPN)

The virtual private network (VPN) at the University of the Witwatersrand, Johannesburg, extends the Wits network across a public network, such as the Internet. It enables a computer connected to the Internet to send and receive data across shared or public networks as if it were directly connected to the Wits network whilst maintaining functionality, security and management policies.

From a user perspective, the extended network resources are accessed in the same way as resources available within the Wits network with certain limitations. VPN allows the Wits community to securely access the intranet and other resources while traveling outside of the University.

Connectivity from the external networks to the Wits University Network is facilitated through the use of (VPN) Virtual Private Network client software. Download the Checkpoint VPN client software from [http://www.wits.ac.za/access](http://www.wits.ac.za/access)

1. The VPN software can be downloaded from: [http://www.wits.ac.za/access](http://www.wits.ac.za/access)
2. Download and save the software onto your local hard drive.
3. 

![VPN software download interface](image)
SECTION B6.1 - WINDOWS 7 & 8 CHECKPOINT VPN

Windows XP is no longer be supported due to Microsoft support policy.

Double click on the installation file and Click on “Next”

Select SecuRemote and click on “Next”

Accept the licence agreement terms and click on “Next”
Click on Install

Click on Finish
Restart your desktop/laptop by selecting Yes, you will be notified that the site configuration is not done and be asked to create one. Click “Yes”

Start the Site Wizard and Click Next
NB: for Windows 8 follow instructions below from Section B 6.2

Insert vpn.wits.ac.za in the field labelled Server Address or Name

Click on “Next”

Click on Trust and Continue
Select Username and Password option for Authentication Method. Click on "Next"

**Students:**
Username: Students/Student No.
Password: Password allocated on registration

**Staff:**
Username: DS\Staff No.
Password: Email Password

**SECTION B6.2 - WINDOWS 8 CHECKPOINT VPN**

Follow steps for downloading as per Windows 7 until you get to the Installation Wizard complete and VPN Installer Information dialogue box.

Once your device has rebooted, locate the installed Check Point VPN software from the Start menu and open it.
Follow the instructions as per below to configure:
Click **Yes** than Click **Next**

Type the following in the **Server address or Name** field: Vpn.wits.ac.za, and click **Next**. Wait for a new profile to be created as per dialogue box below:

Click on **Trust and Continue** Select **Username and Password** and click **Next**.
SECTION B6.3 - VPN FOR APPLE MAC

Go to www.wits.ac.za/access, and from the Mac section, download and open the zip file. Once the zip file is open, you will see the following 3 files.

Open the Tunnelblick dmg file.
Double click the **Tunnelblick** icon to begin installation.

Enter your **MacBook username and password** to authorize the installation and click **ok**.

Click **Launch**
Click on I have configuration files.

Select Done.

Navigate back to the 3 files that were extracted from the Zip file. Open the ovpn file.

Select Only Me.
Enter your **MacBook username** and **password** and click **ok**.

You will see a new icon on the top right of the Menu bar, click this icon and select **Connect ea1bq_551810014037771164**.

<table>
<thead>
<tr>
<th>Students</th>
<th>Staff</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username: Students/Student No.</td>
<td>Username: DS\Staff No.</td>
</tr>
<tr>
<td>Password: Password allocated on registration</td>
<td>Password: Email Password</td>
</tr>
</tbody>
</table>
You are now connected to the VPN.

This concludes the configuration of VPN for Mac machines.

SECTION B6.4 - VPN ON UBUNTU

SECTION B6.4.1 Setting up OpenVPN client on Ubuntu

In this document, the installation and configuration instructions for the Wits OpenVPN have been tested on Lucid Lynx 10.04 LTS, Precise Pangolin 12.04 LTS and Trusty Tahr 14.04 LTS. There should be uniformity and continuity with the other Ubuntu releases. Set up instructions include both CLI (command line interface) and GUI (graphical user interface) methods below.

CNS Help Desk (telephone): 011.717.1717 (or ext 71717 internal call) CNS Help Desk (email): ITHelp@Wits.ac.za
Document version: 1.1
Document release date: 2014.07.03
Document update date: 2014.10.14
Author: Stuart Murray-Smith
Department: CNS InfoSec
Email address: admin@Wits.ac.za

Please report any errata to the InfoSec admin email address above.
SECTION 6.4.1A Install OpenVPN client using the CLI

Assumptions:
- that you know the system administrator password
- that you have downloaded and unzipped the Wits OpenVPN zip file to access this document
- the unzipped folder that contains this document also contains the files: client.ovpn
  WitsVPN.crt
  WitsVPN.ovpn
  WitsVPN.tls
- that when working in a terminal shell, the working directory is this unzipped folder mentioned above

CLI-1
Open a terminal shell, and as system administrator, at the command line run: `sudo apt-get install openvpn`
You will be required to acknowledge that you want to continue by typing 'y' and enter

username@username-VirtualBox:~$ sudo apt-get install openvpn [sudo] password for username:
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following package was automatically installed and is no longer required:
  Linux-image-generic
Use `apt-get autoremove` to remove it.
The following extra packages will be installed: libpkcs11-helper1
Suggested packages: easy-rsa
The following NEW packages will be installed: libpkcs11-helper1 openvpn
  0 upgraded, 2 newly installed, 0 to remove and 0 not upgraded. Need to get 423 kB of archives.
  After this operation, 1 159 kB of additional disk space will be used. Do you want to continue? [Y/n] y
  Fetching files ...
  Preconfiguring packages ...
  Selecting previously unselected package libpkcs11-helper1:amd64. (Reading database ... 193353 files and directories currently installed.) Preparing to unpack .../libpkcs11-helper1_1.11-1_amd64.deb ... Unpacking libpkcs11-helper1:amd64 (1.11-1) ...
  Selecting previously unselected package openvpn.
  Preparing to unpack .../openvpn_2.3.2-7ubuntu3_amd64.deb ... Unpacking openvpn (2.3.2-7ubuntu3) ...
  Processing triggers for man-db (2.6.7-1) ... Processing triggers for ureadahead (0.100.0-16) ...
  ureadahead will be reprofiled on next reboot Setting up libpkcs11-helper1:amd64 (1.11-1) ...
  Setting up openvpn (2.3.2-7ubuntu3) ...
  * Restarting virtual private network daemon(s)...

CLI-2
If you would prefer to set up your Wits VPN connection using the GUI (graphical user interface), but would like to install the OpenVPN Network Manager package using your existing open terminal shell, as system administrator, at the command line, type:

`sudo apt-get install network-manager-openvpn`

Skip the subsequent CLI steps and go to GUI-1 (you may close or minimise your terminal shell now)
username@username-VirtualBox:~$ sudo apt-get install network-manager-openvpn
Reading package lists... Done
Building dependency tree Reading state information... Done
The following package was automatically installed and is no longer required: linux-image-generic
Use `apt-get autoremove` to remove it.
The following extra packages will be installed: network-manager-openvpn-gnome
The following NEW packages will be installed:
  network-manager-openvpn network-manager-openvpn-gnome 0 upgraded, 2 newly installed, 0 to
remove and 1 not upgraded. Need to get 152 kB of archives.
After this operation, 1 377 kB of additional disk space will be used. Do you want to continue?

[Y/n] y
Get:1 http://za.archive.ubuntu.com/ubuntu/trusty/universe network-manager-openvpn amd64 0.9.8.2-1ubuntu4 [21.4 kB]
Get:2 http://za.archive.ubuntu.com/ubuntu/trusty/universe network-manager-openvpn-gnome amd64 0.9.8.2-1ubuntu4 [131 kB]
Fetched 152 kB in 0s (171 kB/s)

Selecting previously unselected package network-manager-openvpn. (Reading database ... 193429 files and directories currently installed.)
Preparing to unpack .../network-manager-openvpn_0.9.8.2-1ubuntu4_amd64.deb ... Unpacking network-manager-openvpn (0.9.8.2-1ubuntu4) ...
Selecting previously unselected package network-manager-openvpn-gnome.
Preparing to unpack .../network-manager-openvpn-gnome_0.9.8.2-1ubuntu4_amd64.deb ... Unpacking network-manager-openvpn-gnome (0.9.8.2-1ubuntu4) ...
Setting up network-manager-openvpn (0.9.8.2-1ubuntu4) ...
Setting up network-manager-openvpn-gnome (0.9.8.2-1ubuntu4) ...
username@username-VirtualBox:$

CLI-3 Rename and move the Wits VPN configuration file to the OpenVPN configuration path:

ls -al /etc/openvpn/ && sudo mv client.ovpn /etc/openvpn/client.conf && ls -al /etc/openvpn/ &&
You may notice that client.conf has been added to the /etc/openvpn directory
username@username-VirtualBox:$

CLI-4 To start the OpenVPN client, at the command prompt type: sudo service openvpn start
The startup process will ask for your AD credentials, type your AD user ID (example used below):

DS\A0012345
and press enter, followed by your password, and press enter again. username@username-VirtualBox:$
sudo service openvpn start
Starting virtual private network daemon(s)...
* Autostarting VPN 'client'
Enter Auth Username:DS\A0012345 Enter Auth Password:
To check the status of OpenVPN client:
```
sudo service openvpn status
```
* VPN ‘client’ is running

To stop OpenVPN client, type this at the command prompt:
```
sudo service openvpn stop
```
* Stopping virtual private network daemon(s)...  * Stopping VPN ‘client’     [ OK ]

SECTION B6.4.1B Install OpenVPN client using the GUI

Assumptions:
- that you know the system administrator password
- that you have downloaded and unzipped the Wits OpenVPN zip file to access this document
- the unzipped folder that contains this document also contains the files: `client.ovpn`
- `WitsVPN.crt` `WitsVPN.ovpn` `WitsVPN.tls`
- that when working in a terminal shell, the working directory is this unzipped folder mentioned above
- that the package `network-manager-openvpn` (and all its dependencies) has already been installed

**GUI**
Left-click the Network Manager icon (counter-pointing arrows, assuming you have wired network connectivity) on the applets panel, slide the mouse arrow down to ‘VPN Connections,’ slide the mouse arrow across and left-click on ‘Configure VPN.’
GUI-2  Left-click 'Add' to create a new connection (this time, it’s a VPN connection)

GUI-3  Lucid Lynx 10.04 LTS and Precise Pangolin 12.04 LTS releases provide this dialog box. Left click on 'Import' and go to GUI-6
GUI-4 Trusty Tahr 14.04 LTS release provides this dialog box. Left-click the drop-down box and and select 'Import a saved VPN configuration.' by left-clicking on it.

GUI-5 Left-click 'Create...'

GUI-6 Navigate to the directory where you extracted the WitsVPN.zip file, select the WitsVPN.ovpn file, and left-click 'Open'
GUI-7  Importing the saved configuration isn’t an exact fit. We have to alter a few of the input fields.

GUI-8  Left-click on ‘Certificates (TLS)’ and select ‘Password’
GUI-9  Selecting 'Password' changes the input fields. Enter your AD user ID (example used below) in the 'User name' field, and AD password in the 'Password' field. Left-click on 'CA Certificate' to select the WitsVPN CA cert.

GUI-8  Left-click on 'Certificates (TLS)' and select 'Password'.
GUI-9  Selecting 'Password' changes the input fields. Enter your AD user ID (example used below) in the 'User name' field, and AD password in the 'Password' field. Left-click on 'CA Certificate' to select the WitsVPN CA cert.

GUI-10  Navigate back to the directory where you extracted the WitsVPN.zip file, select the WitsVPN.crt file, and left-click 'Open'

GUI-11  Left-click on 'Advanced' at the bottom right
GUI-12 Under the 'General' tab, ensure that 'Use LZO data compression' is checked
GUI-13 Left-click the 'TLS Authentication' tab and check the 'Use additional TLS authentication' checkbox

GUI-14 Left-click '(None)' to the right of 'Key File:' to load the WitsVPN TLS key file

GUI-15 Navigate to the directory where you extracted the WitsVPN.zip file, select the WitsVPN.tls file, and left-click 'Open'
GUI-16 Left-click the blank drop-down box to the right of ‘Key Direction’ to select key direction.
GUI-17 Left-click on ‘1’

GUI-18 Left-click ‘OK’ at the bottom right
GUI-19 Left-click 'Save...' at the bottom right

GUI-20 You should see that the WitsVPN connection has been created (and that it has 'never' been used). Left-click 'Close' at the bottom right

GUI-21 Now to test the newly created VPN connection. Left-click the Network Manager icon (counterpointing arrows, assuming you have wired network connectivity) on the applets panel, slide the mouse arrow down to 'VPN Connections,' slide the mouse arrow across and left-click on 'WitsVPN.'
GUI-22 You should see confirmation that you have logged in successfully. If not, contact CNS Service Desk at the contact details above.

GUI-23 To check if your established WitsVPN connection is (still) active, left-click the Network Manager icon (counter-pointing arrows, assuming you have wired network connectivity) on the applets panel, slide the mouse arrow down to ‘VPN Connections,’ slide the mouse arrow across and highlight ‘WitsVPN.’ If you are connected to WitsVPN, a little tick mark will appear to the left of ‘WitsVPN’.
SECTION B7 - PROXY SETTINGS

SECTION B7.1 - PROXY SETTINGS ON WINDOWS INTERNET EXPLORER

Open internet explorer, click ‘tools, internet options’

Click ‘Connections, LAN Settings’

Change the address to:

Students:  proxyss.wits.ac.za - port 80,
Staff:  proxyad.wits.ac.za – port 80

Open a new page and it should ask for a username and password for proxyss.wits.ac.za/proxyad.wits.ac.za which would be as below:

Username would be students’ student number with a capital letter in the student number, or Staff number and password

Use your email password as your proxy password as well.
SECTION B7.2 - PROXY SETTINGS FOR FIREFOX/MOZILLA

From within Firefox, click on "Open Menu" and then "Options".

Click on "Advanced" and then "Settings".
For Students:

You can now start browsing the internet. When the “Authentication Required” window pops up, use students\student number as the “User Name” and your student email password, as the “Password”.

![Authentication Required dialog](image-url)
For Staff members:

You can now start browsing the internet. When the “Authentication Required” window pops up, use DS\staff number as the “User Name” and your staff email password, as the “Password”.

NB.

<table>
<thead>
<tr>
<th>Students</th>
<th>Staff</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username: Students/Student No.</td>
<td>Username: DS\Staff No.</td>
</tr>
<tr>
<td>Password:</td>
<td>Password: Email Password</td>
</tr>
<tr>
<td>Password allocated on registration</td>
<td></td>
</tr>
</tbody>
</table>
SECTION B7.3 - PROXY SETTINGS ON APPLE MAC OS X VERSION 10.3.X

CONFIGURING SYSTEM PREFERENCES IN THE NETWORK PANE

Click on the Apple Menu and select "System Preferences".

Click on "Network" and then highlight whichever network connection you want to configure, and then click on "Advanced".
Make sure that the bypass proxy options are set as in the screenshot and then tick the "Web Proxy (HTTP)" box.
For students: Set the "Web Proxy Server" settings as per the screenshot below.

For staff: Set the "Web Proxy Server" settings as per the screenshot below.
Then Tick the “Secure Web Proxy (HTTPS)
For students: Set the “Secure Web Proxy Server” settings as per the below screenshot

For staff: Set the “Secure Web Proxy Server” settings as per the screenshot below.

Click on “OK”. If you get a message stating “System Preferences wants to use your confidential information stored in the ... in your keychain,” select the “Always Allow” option.
Click on "Apply", and you are done with the configuration.

SECTION B7.4 - PROXY SETTINGS ON APPLE MAC FOR FIREFOX/MOZILLA

From within Firefox, click on "Open Menu" and then "Preferences".
Click on “Advanced” and then under “Network” click on “Settings”.

For Students:

Click “OK”. You can now start browsing the internet. When the “Authentication Required” window pops up, use student's student number as the “User Name” and your student email password, as the “Password”.
For Staff:

Click "OK". You can now start browsing the internet. When the “Authentication Required” window pops up, use DS\staff number as the “User Name” and your staff email password, as the “Password”.

Version 8.0.1 2016
SECTION B8 - WIRELESS ACCESS FOR LAPTOPS AND NOTEBOOKS

SECTION B8.1 - WIRELESS SETUP FOR WINDOWS 8

Right click on the network connection status icon (located on the task bar – bottom right corner of your screen just next to the time) and right click on it. Choose the “Open Network and Sharing Center” option.

Click on the “Set up a new connection or network” option as seen in the screen shot below:

Choose the “manually connect to a wireless network” option and click “Next”.

Configure The SSID as per screen shot below:
Network Name: Wits-Wifi [please note that both W’s must be in capital letters].
Security type: WPA-Enterprise
Encryption type: AES
Then click on “Next”
Then click on “change connection settings” in the next screen that will appear as seen below:

Select the “Security” tab at the top. Uncheck the “remember my credentials for the connection each time I’m logged in” and then click on the “settings” button as seen below:

Uncheck “Verify the Servers identity by validating the certificate” and click on the “Configure” button as seen in the screen shot below.

After clicking on the “Configure” button as seen in the screen shot above, the following window will pop (screen shot below). Uncheck the option below as seen in the screen shot and click on “OK” and that should bring you back to the screen shot above. Click on the “OK” to close the “Protected PEAP Properties window”.

Then click on “change connection settings” in the next screen that will appear as seen below:

Select the “Security” tab at the top. Uncheck the “remember my credentials for the connection each time I’m logged in” and then click on the “settings” button as seen below:

Uncheck “Verify the Servers identity by validating the certificate” and click on the “Configure” button as seen in the screen shot below.

After clicking on the “Configure” button as seen in the screen shot above, the following window will pop (screen shot below). Uncheck the option below as seen in the screen shot and click on “OK” and that should bring you back to the screen shot above. Click on the “OK” to close the “Protected PEAP Properties window”.

Uncheck “Verify the Servers identity by validating the certificate” and click on the “Configure” button as seen in the screen shot below.

After clicking on the “Configure” button as seen in the screen shot above, the following window will pop (screen shot below). Uncheck the option below as seen in the screen shot and click on “OK” and that should bring you back to the screen shot above. Click on the “OK” to close the “Protected PEAP Properties window”. 
The screen shot below will appear. Click on the “Advanced Settings” button.

Check the “specify authentication mode” and click on the “Save Credentials” button and then choose the “User Authentication” option from the list as seen in Fig.1. An authentication tab will appear as seen in Fig.2.
Please take note of the following:

<table>
<thead>
<tr>
<th>Students</th>
<th>Staff:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username: Students/Student No.</td>
<td>Username: DS\Staff No.</td>
</tr>
<tr>
<td>Password:</td>
<td>Password: Email Password</td>
</tr>
<tr>
<td>Password allocated on registration</td>
<td></td>
</tr>
</tbody>
</table>

This should bring you to the screen as per screen shot below. Click on the “Close” button to complete the setup.

When you are done with configuring the “Wits-Wifi” wireless network, you can now connect to it as illustrated in the figure below. Go to your “Network” icon and click on it. It should list all the available wireless networks. Choose Wits-Wifi and connect to it as illustrated in the screen below. Please make sure that the “Connect Automatically” is checked.
The last thing you will need to do in order to be able to browse the internet, is to configure your Internet proxy settings. This is done in your internet browser, for instance Internet Explorer or Mozilla Firefox. Please note that if you are using Google Chrome, you will need to setup the Internet explorer and Google Chrome will derive the settings from IE.

Step 13: Internet Explorer Or Google Chrome Users: Open Internet explorer, in the top section, go to Tools, and then choose “Internet Options” as seen in the screenshot below.
A window like the one in the screen shot below will appear. Click on the “Connections” tab and click on the “LAN settings” button.

This will bring up the following window (Fig. 5). Make sure you have both of the options in the proxy server section checked as seen in the screen shot below (Fig.5).

For students: The Proxy Server must be proxyss.wits.ac.za and Port: 80
For Staff: The Proxy server must be proxyad.wits.ac.za and Port: 80

When you have done this, click on the “Advanced” button and a window as seen in Fig6 above will appear. You will then need to insert the following in the text field provided: *.wits.ac.za;146.141. *

Step 16: Mozilla Firefox Users: Open your internet browser. Go to “tools”, and then go to “options” like in the screen shot below.

Go to “Advanced”, choose the “network” tab, and then click on the “settings” button like in the screen shot below.
Insert as in the screen shot below, check the “manual proxy configuration” and set the “HTTP proxy” as follows:

**Staff members:** proxyad.wits.ac.za Port: 80  
**Students:** proxyss.wits.ac.za Port: 80

You will then need to check “use this proxy for for all protocols” option like in the screen shot below.

At "No proxy for" type insert *.wits.ac.za,146.141.*

When you are done with all these settings, click on OK and you are ready to browse the Internet.
SECTION B8.2 - WIRELESS SETUP FOR WINDOWS 7

Click "start", go to "control panel", and then select "network and sharing center". Choose the 1st option, "set up a new connection or network" as seen in the screen shot below:

Choose option 3 "Manually connect a wireless network" and then click "Next"

Configure The SSID as per screen shot below:
Network Name: Wits-Wifi (please note that both W’s must be in capital letters).
Security type: WPA-Enterprise
Encryption type: AES
Then click on "Next"
Then click on “change connection settings” in the next screen that will appear as seen below:

Select the “Security” tab at the top. Uncheck the “remember my credentials for the connection each time I’m logged in” and then click on the “settings” button as seen below:

Uncheck “Validate Server certificate” and click on the “Configure” button as seen in the screen shot below.

After clicking on the “Configure” button as seen in the screen shot above, the following window will pop (screen shot below). Uncheck the option below as seen in the screen shot and click on “OK” and that should bring you back to the screen shot above. Click on the “OK” to close the “Protected PEAP Properties window”.

The below screen shot below will appear. Click on the “Advanced Settings” button.

Check the “specify authentication mode” and click on the “Save Credentials” button and then choose the “User Authentication” option from the list as seen in Fig.1. An authentication tab will appear as seen in Fig.2. Please take Note of the following:

For Staff Members: The username will be ds\Staff Number, the password will be your Logon Password.

For Students: The username will be students\Student Number, the password will be your Logon Password.

Enter your credentials and click on the “OK” button.
This should bring you to the screen as per screen shot below. Click on the “Close” button to complete the setup.

Now connect to the Wits-Wifi wireless network as illustrated below. First go to your wireless network icon. Click on it and that should list all available wireless network. Choose Wits-Wifi and click on the “Connect” Button as seen below.

The last thing you will need to do, in order to be able to browse the internet, is to configure your Internet proxy settings. This is done in your internet browser, for instance Internet Explorer or Mozilla Firefox. Please note that if you are using Google chrome, you will need to setup the Internet explorer and Google Chrome will derive the settings from IE.

<table>
<thead>
<tr>
<th>Students</th>
<th>Staff:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username: Students/Student No.</td>
<td>Username: DS\Staff No.</td>
</tr>
<tr>
<td>Password:</td>
<td>Password: Email Password</td>
</tr>
<tr>
<td>Password allocated on registration</td>
<td></td>
</tr>
</tbody>
</table>
SECTION B8.3 - INTERNET EXPLORER OR GOOGLE CHROME USERS

Open Internet explorer, in the top section, go to Tools, and then choose “Internet Options” as seen in the screenshot below.

A window like the one in the screenshot below will appear. Click on the “Connections” tab and click on the “LAN settings” button.

This will bring up the following window (Fig. 5). Make sure you have both of the options in the proxy server section checked as seen in the screenshot below. (fig.5)
SECTION B8.4 - WIRELESS SETUP FOR MOZILLA FIREFOX USERS

Open your internet browser. Go to "tools", and then go to "options" like in the screen shot below.

Go to “Advanced”, choose the “network” tab, and then click on the “settings” button like in the screen shot below.
Insert as in the screen shot below, check the “manual proxy configuration” set the “HTTP proxy” as follows:
Staff members: proxyad.wits.ac.za Port: 80
Students: proxyss.wits.ac.za Port:80
You will then need to check “use this proxy for all protocols” option like in the screen shot below.
At “No proxy for” type *.wits.ac.za,146.141.*

When you are done with all these settings, click on OK and you are ready to browse the Internet.

SECTION B8.5 - WIRELESS ACCESS FOR APPLE MAC AIRPORT,

APPLE MAC OS X MOUNTAIN LION
Please note that the following guide is for connecting to the Wits network via Airport and not via Ethernet. Please make sure that your Wi-Fi is turned on and follow this guide.

NB. The proxy configuration may need to be done in various applications depending on which web browser you are using.

The supported web browsers in this guide are Safari, Firefox, Opera, Camino and Google Chrome.

If you are using Camino or Google Chrome, please follow the Safari instructions. Once you have completed the configuration and you open either Camino or Google Chrome and visit a web site you will be prompted for authentication and need to enter your credentials as:

<table>
<thead>
<tr>
<th>Students</th>
<th>Staff:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username: Students/Student No.</td>
<td>Username: DS \ Staff No.</td>
</tr>
<tr>
<td>Password:</td>
<td>Password: Email Password</td>
</tr>
<tr>
<td>Password allocated on registration</td>
<td></td>
</tr>
</tbody>
</table>
SECTION B8.6 - SAFARI

Wireless Setup for Mac

Note: This document was created using a Mac that was running Mac OS X 10.10.5.

Click on the Wi-Fi icon and select Turn Wi-Fi On.

Select the Wi-Fi icon again and choose Wits-Wifi.

For staff: log in with DS\staff number and your email password. Click on Join.
For Students: log in with STUDENTS\student number and your email password. Click on Join.

Click on Continue.

Type in your Mac’s Admin Username and Password, and click on Update Settings.

Click on the Wi-Fi icon again and select Open Network Preferences.
Make sure that **Wi-Fi** is selected and that the **Network Name** is **Wits-Wifi** and then click on **Advanced.**
Click on the **Proxies** tab.

Tick **Web Proxy (HTTP)** and then under the **Bypass proxy settings for these Hosts and Domains** section add ". wits.ac.za, 146.141. *" and under **Web Proxy Server** put in `proxys.wits.ac.za` for students or `proxyad.wits.ac.za` for staff. The port must be 80. Tick the **Proxy server requires password** option and all students, type in `STUDENTS\student number` as the **Username** and enter your email password as the **Password**. For Staff members: type in `DS\staff number` as the **Username** and your email password.
Tick Secure Web Proxy (HTTPS) and then under the Bypass proxy settings for these Hosts and Domains section add *\.wits\.ac\.za, 146.141. * and under Secure Web Proxy Server put in proxyss\.wits\.ac\.za for students or proxyad\.wits\.ac\.za for staff. The port must be 80. Tick the Proxy server requires password option and all students, type in STUDENTS\student number as the Username and enter your email password as the Password. For staff members: type in DS\staff number as the Username and your email password. Once done, click on OK.

Click on Apply.
Close the last window.

This concludes the configuration for Wireless on a Mac.

SECTION B8.7 - WIRELESS ACCESS FOR LINUX(UBUNTU)

Locate the Desktop of Ubuntu 12.04 LTS

Locate the Network Manager icon in the top, far-right hand corner of the screen
Select the Network Manager icon and then select “Wits-Wifi”

For the Wireless Authentication window, change only the “Authentication” drop-down menu from “Tunneled TLS” ...

Students
Username: Students\Student no
Password: password allocated
Proxy: proxyss.wits.ac.za

Staff
Username: Ds\Staff Number
Password: Email Password
Proxy: proxyad.wits.ac.za

Enter the password associated with you. Then click “Connect” to continue the Wireless setup.
Select the “Don’t warn me again” checkbox, for the Network Manager’s Certificate Authority window, then Click “Ignore” to add the Wireless configuration, without need of a certificate.

The connection will begin to establish, as evident in below. Once a connection has been established, the signal strength will be seen on the Network Manager icon.
SECTION B9 - WITS MOBILITY – SMARTPHONES ETC

Wits offers wireless network coverage on campus to both staff and students. To see the current status of coverage across all Wits campuses you can access a table listing the buildings covered by clicking on https://www.wits.ac.za/mywits/wifi-hotspots/ and more information regarding WiFi use on campus.

The WITS-WIFI-MOBILE Wireless Network is designed for tablet, phablets and smartphone devices. Before you can proceed with the configuration guide below to register your devices; you will need the following information:

- Username – This is your Student or Staff Number at the University.
- Password – This is the same password you use to access University resources e.g. Internet, Email, etc.
- wireless network card address (MAC address) of your tablet, phablet or smartphone device

N.B.
See section B–9.2 below if you are registering a replacement device, only 2 devices may be registered at any one time.

SECTION B – 9.1 CONFIGURING YOUR DEVICE ON THE WITS WI-FI NETWORK

Please note that this guide was created on an Android Device running version 4.4.2. So some screens might appear differently depending on the device you are using.

To locate the MAC Address of your iPad or iPhone:
- Tap Settings.
- Select General.
- Select About.
- The Mac address is listed as Wi-Fi Address

To locate the MAC Address of your Android phone or tablet:
- Press the Home button at the bottom of the phone.
- Press the Menu button.
- Tap Settings.
- Tap Wireless & Networks.
- If Wi-Fi is not already selected, tap Wi-Fi to turn it on.
- Press the Back button.
- Tap About Phone.
- Tap Status.
- Scroll down until you locate the Wi-Fi MAC address

To locate the MAC Address of your BlackBerry Device Software 4.5 to 5.0:
- From the home screen, click Options > Status.
- The WLAN MAC field displays the MAC address for the smartphone.

To locate the MAC Address of your BlackBerry Device Software 6 to 7.1:
- From the home screen, select Setup > Options > Device > Device and Status Information.
- The WLAN MAC field displays the MAC address for the smartphone.
To locate the MAC Address of your BlackBerry OS:

- From the home screen select Settings > Network Connections > Wi-Fi > Advanced.
- In the Diagnostic Information drop-down, select Device Information.
- The Physical Address field displays the MAC address for the smartphone.

To locate the MAC Address of your Windows Mobile Device:

- On Start, flick left to the App list.
- Tap Settings.
- Tap About.
- Tap More info.
- Note the MAC Address.

On your phone navigate to > Settings > Wi-Fi and ensure your wireless network is switched on. Connect to the Wits-WiFi-Mobile wireless network as shown below.

On some devices you will get a pop up asking you to sign in. On other devices you will need to open up your web browser to start browsing to a website. When you attempt to browse, you will get the screen below providing you with information regarding this wireless service. Please read carefully.
Tap the web link, shown below, located towards the end of the information screen.

Please follow this link to register your Mac address

The screen shown below will appear.

![Screen shot of registration page]

Complete the information as displayed below taking special care when inputting the following information and then tap > Submit:

- **Username Field** – To be completed with your Student or Staff Number provided by the University. *Please type this in lower case*
- **Password** – This is the same password you use to access University resources e.g. Internet, Email, etc. *Please note that passwords are case sensitive*
- **MAC address** – This is the wireless network card address of your tablet, phablet or smartphone device which is available on your device.
After Tapping > Submit the screen below appears confirming that the Mac Address was successfully added and an account for the device was created.

Click on > Done to begin browsing the internet or using the apps from your mobile device.

If you have any difficulties using the Wits Wifi Mobile Self Registration system, please contact the CNS Information Technology Service Desk for assistance on ext. 71717 or email ithelp@wits.ac.za

NB. YOU will only be allowed to register two (2) devices per student or staff member.

SECTION B – 9.2 REGISTER/DELETE A MOBILE DEVICE VIA A WEB BROWSER

Please ensure your old device is deleted off the network before you add a new device.

Before you can proceed with the configuration guide below to register your devices; you will need the following information:

- Username – This is your Student or Staff Number at the University.
- Password – This is the same password you use to access University resources e.g. Internet, Email, etc.
- Wireless network card address (MAC address) of your tablet, phablet or smartphone device
  - Android: To find the Wifi MAC Address on an Android device, go to Settings, go to More, followed by About device and then click on Status.
  - iOS: To find the Wifi MAC address on an iOS device, go to Settings, followed by General and then select About.

To register a new mobile device

Log into the Ignition Guest Manager by going to:

https://146.141.15.209/GuestManager/provisioner/

Enter your staff or student credentials and then click on the Login button as displayed in screenshot below. Make sure to only use lowercase letters in the User Name.

Staff - Use your staff number and enter your Wits Active Directory / Email password.
Students - Use your student number and your Wits Active Directory / Email password.
Once logged in, to add a new device go to **New**.

In the **MAC Address** textbox, enter the Wi-Fi MAC address of the mobile device. In the **Comments** textbox, enter the make and model of the device. Once done, click on **Submit** as per screenshot below.
Thereafter, you will see the following screen, confirming that the device application was successful.

You will now be able to connect and use the wits-Wi-Fi-mobile network on the newly registered device.

**To delete any mobile devices you have added**

Log into the Ignition Guest Manager by going to:

https://146.141.15.209/GuestManager/provisioner/

Enter your staff or student credentials and then click on the **Login** button as displayed in screenshot below. Make sure to only use lowercase letters in the User Name.

**Staff** - Use your staff number and enter your Wits Active Directory / Email password.

**Students** - Use your student number and your Wits Active Directory / Email password.
Once logged into the **Ignition Guest Manager**, go to **View**.

From this screen you will be able to see all the devices that you have added.

To delete a device, tick the **check box next to the device** and click on the **Delete** button.
At the next window, confirm the action by clicking on OK.

The device has now been deleted.

If you have any difficulties adding or deleting devices from the Mobile Self Service system, please contact the CNS Information Technology Service Desk for assistance on ext. 71717 or email ithelp@wits.ac.za

SECTION B10 - EDUROAM® SERVICE

Wits belongs to the global eduroam® family, and in keeping with international universities allows access to staff and students from other universities to access the Wi-Fi network using the login and password credentials of the originating university.

HOW TO CONNECT TO eduroam® SERVICE ON CAMPUS

Before connecting to the eduroam® wireless network, please note that as per the ‘eduroam® National Policy for South Africa’ document (dated 2013-05-20), the following TCP ports are open:

- HTTP (80) – normal, unsecured website browsing such as CNN.com
- HTTPS (443) – secure website browsing such as internet banking and e-commerce websites
- IMAP (143) – normal IMAP mailbox client-server synchronisation
- IMAP-SSL (993) – secure IMAP mailbox client-server synchronisation using Secure Sockets Layer
- POP (110) – normal POP3 mailbox email fetching
- POP3-SSL (995) – secure POP3 mailbox email fetching using Secure Sockets Layer
- SMTP (465, 587) – Mail Submission Agents (MSAs), variants of legacy SMTP (port 25)
- SSH (22) – Secure Shell, encrypted data communication for remote command-line login
- VPN – Virtual Private Network, various ports for the various protocols

NB. Only publicly accessible Wits resources will be accessible from the eduroam® wireless network. Access is not allowed to Wits internal resources.
Connect to the eduroam® SSID. Once clicked, the user credentials dialog box pops up:

Open a browser to surf the web. When trying to access a web page, the following captive portal web page is presented to you:

Enter your user ID using your full username and domain as per the example below:

- **Visitors:** e.g. `username@your_domain` and enter your password
- **Wits Staff:** `Staff_number@wits.ac.za` and enter your password
- **Wits Students:** `Student_number@students.wits.ac.za` and enter your password

If you see a request to accept a certificate, please accept it.

Wits students and staff on campus using eduroam will only be able to access the ports and services listed in the start of this document. Wits Intranet and other internal Wits sites and services will not be accessible. Please use Wits-Wifi or Wits-Wifi-Mobile instead.
SECTION B11 - ENHANCED IT SERVICES FOR POSTGRADUATE STUDENTS

The University acknowledges that postgraduate students who undertake research for a higher degree qualification require enhanced IT resources to help them successfully complete their studies.

Here are some of the services offered to postgraduate research students:

- Flexible internet options
- Printing subsidy
- Collaboration areas
- High Speed Printing in Post Graduate Labs

Some of these services are automatically granted to postgraduate students. Others have to be approved by the relevant Faculty.

SECTION B12 - FLEXIBLE INTERNET OPTIONS

Post Graduate research students may have different requirements to other students. These students should approach and discuss these with their supervisor who can advise CNS to accommodate these needs.

SECTION B13 - PRINTING SUBSIDY

To assist postgraduate research students with increased printing requirements, Faculties may grant extra printing credit, deposited directly into the student’s printing account. Students need to discuss these printing requirements directly with their supervisor. When a student’s thesis has been examined, any unused subsidy may be withdrawn.

SECTION B14 - COLLABORATION AREAS

Postgraduate research students may request that a collaborative work area be created on the network. A collaboration area is a shared area on the student network drive separate to your H: drive. This area can be configured for access by the research student, supervisor(s), or any other users working with them.

SECTION B15 - ELEARNING

A large selection of free online courses are available to students via eLSI (eLearning Support & Innovation) on the website https://elearn.wits.ac.za via VTC (Virtual Training Courses). This is a collection of training tutorials offered to Wits students as an easy and convenient way to learn new software skills from their desks, working at their own pace.
TRAINING TUTORIALS ARE AVAILABLE IN THE FOLLOWING CATEGORIES:

Graphics & Page Layout,
Business Applications
Multimedia, Video
Internet & Web Design
Operating Systems
Databases, and Programming
Animation & 3D Audio Certification
Networking and Security Project Management
CAD

Detailed information about the courses is provided by tutorials which can be accessed via:
elearn@wits.ac.za

Contact Antoinette Malgas or Lerato Mahlakoleng by email elearn@wits.ac.za for further information and details.

NB. Please adhere to copyright laws and refer to the Acceptable Use policy http://www.wits.ac.za/accept
SECTION C - STAFF ICT SECTION

SECTION C1 - NEW USER CONFIGURATION

Ensure that you have a newly issued unique ‘staff number’ from HR. If the user does not have one, please let them know that CNS do not add staff to the system, it is done by HR by means of an Oracle profile setup. If the user is a Wits staff member, he/she can approach their own HR office to get this. If the user is a Non-Wits staff member, then he/she can fill out this form also found on the Wits intranet:

This document must be sent to central HR at Senate House.

http://intranet.wits.ac.za/itd/itsupport/cns/Pages/Oracle-Access-Request-Form.aspx

Once you have the staff number, the new user can be added to Call Logging profile database as well when the call is logged for the setup of the new user on the pc.

You will receive:
1. An AD (Active Directory) account
2. Email account (email format is Firstname.Surname@wits.ac.za)
3. i-Wits Employee Self Service
4. An inbound fax number.

SECTION C2 - PASSWORD RESET

PASSWORD SELF-SERVICE

NB: In order for staff members to use the Password Self-Service, they have to firstly do a once off registration. The steps for the registration are below. (If you have already registered for the service, you can skip to the section “How to reset your password section further below”.

Registration:

Via an internet browser, go to https://passwordregistration.wits.ac.za.

For the User Name enter ds\staff number and for the Password enter your email password.

If your machine is on the staff domain and you are logged into the domain with your profile, then you will skip this step continue to the next step - Click on Ok.
Click on Next.

Type in your email password and click on Next.

Enter your cell phone number and click on Next.

You are now registered for the Password Self-Service.
HOW TO RESET YOUR PASSWORD:

 Via an internet browser, go to https://passwordreset.wits.ac.za.
Enter ds\staff number or staff number@wits.ac.za and click on Next.

You will then receive an SMS on the cell number that you supplied in the initial registration process above. Type in the security code you received and then click on Next.

Type in a new password of your choice and re-type it, then click Next.
You have now successfully reset your password.

Students note: To get your WITS number, replace the first two digits of your ICAM Number with a "W" and leave out the last two digits, i.e. ICAM "22222222 S2" becomes "W2222222"

and

ICAM "100223467 02" becomes "W023467"

For help on using this password self-service portal: click here.

You should reset your password on receiving it for the first time.
SECTION C3 - EMAIL SERVICES

GROUP DISTRIBUTION OF EMAIL AND MESSENGING - ROCKET MAIL

Marketing provides a service subscribed to RocketSeed which allows you to send an “email blast”/”email shot” to a list of recipient email addresses as a group. Users, e.g. student groups, large group communications e.g. bulk mailing.

There however are variable costs/thousand emails depending on the size of the mail shot. The benefit of the Rocketseed system is that it comes with a full reporting module. One can track the success of the outgoing mail.

Should a dept. wish to send a bulk mail to a select group of people both internal and/or external to WITS, you would need to supply a list of email addresses for the email shot to Marketing. Marketing will then assist with the layout of the email to ensure best practice.

If a department intends to send out mailshots/newsletters regularly, training will be provided in the use of the product.

SECTION C3.1 - EMAIL DISTRIBUTION LIST

MAILMAN - DISTRIBUTION LIST

The mailman distribution list is on server “lists.wits.ac.za (alias jupiter.wits.ac.za)”. This is a service apart from your Outlook distribution list which enables people who want to send out newsletters, etc. to a list of people by sending the message to one address, rather than to individual people.

A distribution list is a group of e-mail addresses, usually grouped under a single e-mail address. When you send to a distribution list, you’re really sending to everyone whose address is included in the list, it’s much easier than picking 30 different addresses from the Address Book.

Example: -

Assume the list CNS contains all the CNS staff members then in order to send a message to everyone a message would be sent to cns@lists.wits.ac.za or to cns@jupiter.wits.ac.za

This would allow everyone subscribed to the above list to receive the message.

The distribution list also allows discussions where every person on the list is allowed to send a message to the list.

If the list has too many members (over 500 members) then we try to prevent discussions by allowing only the owner or administrator of the list to send messages to the list.

Technically all the list server does is once it receives an email for a list it passes it back to the wits mail server with the individual email addresses for all the list members.

It doesn't scan or change the mail in anyway, it just reroutes it.

It works exactly the same as the windows distribution list except that it allows all email addresses (internal and external to wits) whereas the windows distribution list only distributes to wits staff.
The first illustration circled in a red indicates who the Owner of the list is. This means only this person is able to modify (add or remove) members from this list.

1. Illustrates the current list of actual members.
2. Allows you to modify the members as in the 1st point.
3. Email addresses shows you the actual email address aliases.
4. Shows you the Global Address Book group name format.

SECTION C3.2 - MODIFYING AND MANAGING (ADDING/REMOVING) MEMBERS TO THE LIST

These are lists which are created in a share for use by departments or dedicated groups e.g. #Comm-KIMi-Comms. Select the options as displayed in the image above, to add members you will be directed to the GAL (Global Address List) to select the new members and to Remove a member you click and remove, the name just disappears from this list.

Finding the Group name on the GAL (Global Address List)

Type # followed by the word ‘Dept’ then type in the dept name of the group you’re searching for e.g. CNS as in the above distribution group example. You can then complete the search by either searching the list of options that come up or you can search the list name if you know it.

To find a single user name

You can type in the first few letters of the name, for e.g. as in the below illustration: ‘faiz’ then click on the control then k buttons on the keyboard for a complete list of possible name.

![Image of email interface](image)

You may also click on the To... field and type the same example name to see a list of all the persons and lists with this name formats.

SECTION C3.3 - SETTING UP A SHARED MAILBOX

An email mailbox is a directory that stores messages for a single user or email address. An email mailbox (also email box, e-mail box) is the equivalent of a letter box for electronic mail, it is where electronic mail messages are delivered. These are used by departmental Administrators and Personal Assistants managing multiple email mailboxes.
How to add a shared/departmental mailbox to your outlook profile in Outlook ver X

In Outlook on File and then click on the icon Account Settings

Next Click on Account Settings again

Select the mail setup tab and click the E-mail accounts button

Select the email account and click on change.
Select the Advanced tab and click on Add.

Enter the name or email address of the mailbox you would like to view and the click on OK and OK again.

Click on Next and then Finish.
SECTION C3.4 - ADD A SHARED MAILBOX ON A SEPARATE OUTLOOK PROFILE

This is the recommended method of setting up departmental mailboxes as it will keep all mail together regarding each mailbox (e.g., sent items/deleted items) as opposed to having both mailboxes under one profile which will then move sent items which you sent on behalf of the departmental mailbox as an example under your personal emails sent items etc.

EMAIL MAILBOX ACCESS

To gain access to another user’s mailbox you are required to log a call with the Staff Service Desk or email ithelp@wits.ac.za You will be guided through the relevant procedure.

Make sure Microsoft Outlook is closed then click on Start and select the Control Panel.

Under the Control Panel double click on Mail.
Click on the **Show Profiles** button.

Click on **Add**.

Type the Name of the departmental mailbox under **Profile Name**.

Select the **Manually configure server setting or additional server types** option.
Select Microsoft Exchange or compatible service.

Type the following in the corresponding fields:
Server: Clymene.ds.wits.ac.za
User Name: Departmental Mailbox Name or E-mail Address
Click on Check Name and then Next.

Click on Finished.

Before clicking on OK make sure that Prompt for a profile to be used option is selected otherwise you will not be able to choose which Outlook profile to open and Outlook will open the same default profile everytime.
You will need to have rights to view the mailbox/folders within the mailbox. If you have setup a departmental mailbox under your own outlook profile and would like to send mail on behalf of the departmental mailbox, you will have to apply for send on behalf of rights. You can request any of this by logging a call with CNS to have rights given to view/send on behalf of the requested mailbox.

SECTION C3.5 - HOW TO ADD A SHARED/DEPARTMENTAL MAILBOX IN OUTLOOK 2016 ON AN APPLE MAC

How to add a shared/departmental mailbox in Outlook 2016 on a Mac

Open Outlook 2016, via the finder, desktop shortcut or search bar.
From the menu bar, click on **Outlook** and then **Preferences**…

From the **Outlook Preferences** section, open **Accounts**.

From within **Accounts**, click on **Add an account**, and then on **Exchange**…
Type in the E-mail address field type in the shared/departmental mailbox name. Under Authentication, type in DS\your staff number and your Wits staff email password. Lastly, click on Add Account.

You will now see the newly added shared mailbox account in the list of accounts. The status light might show orange for a while, until the mailbox has fully synced. After the sync, it will show green, confirming that it is configured correctly. If desired, you can also change the account description here, in case you want to differentiate it more from any other mailboxes that are already added. Once done, you can close the Accounts window.
In the Outlook folder list on the left, you will now notice that the newly added shared mailbox’s inbox, will be appearing under the Inbox section, and all of the shared mailbox’s other folders will be listed under the shared mailbox name below.

SECTION C3.6 - HOW TO SEND A MAIL ON BEHALF OF A DEPARTMENTAL MAILBOX. (SAME PROFILE)

Before sending a new mail, make sure the from field is shown by clicking on options tab and selecting the from button as shown below.
In the **from** field, drop down the list and select the departmental mailbox.

Now when the recipient receives the email, it will state your name on behalf of the mailbox.

**SECTION C3.7 - HOW TO ACCESS A DEPARTMENTAL MAILBOX VIA WEBMAIL.**

**How to open or view a shared mailbox from Outlook Web Access**

Browse to https://email.wits.ac.za/owa

Sign in with your staff number and email password.

---

**Microsoft**

**Outlook Web App**

Security (show explanation)

- This is a public or shared computer
- This is a private computer

1. Click on the light version of Outlook Web App

User name: **staff number**

Password: ***********

Connected to Microsoft Exchange
© 2010 Microsoft Corporation. All rights reserved.
Once signed in, click on your display name in the top right corner, and in the select mailbox: section, type in the primary name of the shared mailbox, and then click twice on Open…

You will now see that the mailbox name on the left will be showing the shared mailbox name, and the mail displayed in the Inbox, will be displaying the mail from the shared mailbox.

Once you are done viewing the shared mailbox, to view your personal mailbox again, you can either sign out and sign back in, or while you are still signed in, follow step 2 above again, but this time type in your name and surname (instead of the shared mailbox).
SECTION C3.8 - HOW TO GIVE ANOTHER USER VIEW PERMISSIONS ON A DEPARTMENTAL MAILBOX.

This will only allow the user to view the selected folders within the mailbox, if you would like the user to send on behalf of the mailbox, a call with CNS will have to be logged requesting such rights for the user.

In Outlook, **Right click** on the name/email address of the mailbox and select **properties**.

Select the **Permissions** tab and click on **Add**.
Enter the name of the user or search for it in the GAL for who you would like to give permissions to and then click on **Add** and then **OK**.

Under **Permission Level** select the type of rights you would like to assign, usually **Reviewer** rights are sufficient for the user to access the mailbox, once selected Click on **OK**.

You will have to repeat the same step for each folder you would like the user to have viewership/access to, eg: Right click on **Inbox** and edit the properties for the inbox as you did the mailbox/email address, see below.
There are a number of options available to you when you require a non-person or “function/service”-related email addresses.

SECTION C3.9 - SHARING CALENDERS AND GRANTING ACCESS

CNS provides an integrated email and calendaring environment. Managers can share their calendar, and email and/or email rights with their secretary or teams can share their calendars. Even without calendar sharing Free/Busy times for staff are shown in the calendaring system. You can block out portions of your diary using recurring entries, for example booking lunchtimes for the whole year in one calendar definition. Lecturers can book tutorials in the CNS labs through the Global Address List (GAL).

The format on the GAL for such lab calendars is: #dept-CNS-Labname.

SECTION C3.10 - EMAIL SOFTWARE

CNS provides enterprise level email to all staff. Currently the main email client that is supported is Outlook Ver. X. Users can also connect to the email server using IMAP, which is the recommended method for Linux and Apple Mac users.

You can access your email through the web anywhere in the world, by going to: https://email.wits.ac.za/owa

SECTION C3.11 - EMAIL MAILBOX SIZE INCREASE

The default email box size allocated to you as the user on the email server is 2GB. Though this could be increased if there is a business requirement for a larger mailbox, this doesn’t however mean that all users (or even most) should have large email boxes. An application form is available from the Service desk if required. Regardless of the size of the mailbox, you would still need to archive your email to your local PC to the “C:\My Mail” folder. For assistance to archive your email effectively log a call with the CNS Staff Service Desk. (Service Desk staff can assist on guiding with archiving of mail)
SECTION C4 - ORACLE EMPLOYEE SELF SERVICE

The University utilizes Oracle systems to manage HR and Finance systems. The system allows the employee to change personal information as they move from department to department, and manage this information in order that it is always current. You can access the system to change your information personal to you and that which you would want to add as viewable to staff and management.

Below is an example on how to access Forms for all supported services offered via the service desk. You would need to click on the following link and complete the required form:

NB. You would need to be logged on to the University Network online or via VPN on the Intranet to be able to access the link below

[http://intranet.wits.ac.za/gtd/itsupport/cns/Pages/Forms.aspx](http://intranet.wits.ac.za/gtd/itsupport/cns/Pages/Forms.aspx)

REQUESTING ADDITIONAL ACCESS

Staff members in Finance requiring additional access to modules will need to click on the link below and fill in the form to acquire access to the necessary modules

[http://intranet.wits.ac.za/gtd/itsupport/cns/Pages/Forms.aspx](http://intranet.wits.ac.za/gtd/itsupport/cns/Pages/Forms.aspx)

FOR TECHNICAL PROBLEMS – CONTACT:

CNS Service Desk
1st Floor, West Wing, Senate House Building, East Campus
E-mail: ITHelp@wits.ac.za
Or call Tel: 011 717 1717
SECTION C4.1 - CHANGING YOUR OFFICE TELEPHONE NUMBER AND UPDATING INFORMATION ON I-WITS

You will need to logon to the i-WITS Oracle Production system. To do so, click on link or follow the pages illustrated below:

http://intranet.wits.ac.za/Pages/Default.aspx

Then click on Applications http://intranet.wits.ac.za/Pages/QAP-Apps.aspx

Then... https://iwits.wits.ac.za/OA_HTML/RF.jsp?function_id=32749&resp_id=1&resp_appl_id=1&security_group_id=0&lang_code=US&oas=5nL5-98Hvud,YrbdY0A..&params=lqRJg7rHlsO.EaUx6T.byg

This will open the following screen: Enter your Staff Number and password, then click Login.

Click on Wits Employee Self Service, then Personal Information,
Click update in the relevant boxes

Enter your correct telephone numbers in the fields provided, then click next to accept the change.

The approved telephone format is a requirement from SARS:
Example: 0117171717
NOTE: note no spaces, no international dialling format

SECTION C4.2 - SETTING YOUR PREFERRED NAME (EMAIL)
If you have a first name that is different to the name that your colleagues know you by, you could have your email address rather reflect your known/preferred/nick name.

This is due to the fact that the *name on your ID book might be different to the name you are known by.*

For example: Nonhlanhla is actually known as Nona

**Your name on the Oracle system is entered as it appears in your identification document.** Although you cannot change your first name on the Oracle system, you can add a preferred name, which then is the name displayed in your email address. This will make it easy for other people to find you on the Global Address List (GAL)

To do this, you need to logon to the i-WITS Oracle Production web site as above, then …

Click on Update on the Basic Details
Then check Correct or complete the current details, then click Next
Now enter the field **Preferred Name** in the **Name**.

Click **Next** and then **Submit** on the following screen, to receive confirmation of change.

**SECTION C4.2 - E-SERVICES - NEW WEB SITE**

A department or group or individual may require a website for publishing information to the Intranet. Navigate to CNS’s intranet website and Forms to fill in and submit the application form for a new website from the address below:

http://intranet.wits.ac.za/gtd/itsupport/cns/Pages/New-Website-Request-Form.aspx

The form will be submitted to the Web Services team who in turn will contact the user with regards the status of the application etc.

**DOCUMENT PORTAL (SHAREPOINT 2013)**

CNS & Marketing together offer SHAREPOINT 2013, a web based collaboration tool for an internal internet presence to the University user community. This presence includes News and Events with Alerts and Calendaring, a shared library and a departmental library with restricted and secure access. SharePoint 2013 offers a simplified user experience and added enterprise social media capabilities, which expand upon previously offered capabilities for website management that include shared
calendars, blogs, wikis, surveys, document libraries and shared task lists. SharePoint 2013 includes a community forum for users to engage in and categorize discussions, a microblogging capability and enhanced search capabilities.

To apply for a Library portal on SHAREPOINT go to CNS and then Forms from the Intranet and click on:

http://intranet.wits.ac.za/gtd/itsupport/cns/Pages/Sharepoint-Services-Library-Request-Form.aspx

SECTION C4.3 - FAX2EMAIL

CNS offers efficient Inbound & Outbound fax services incorporated with Outlook.

By default, all Wits user receives his/her own personal fax number (inbound, receiving of faxes). This is as secure as an email address and functions in the same manner as an email address. Faxes will be delivered to the email address connected only. Outbound faxing means that a fax can be sent from your pc, in an email message.

An applications and approval process is required for the Outbound fax option, since the HOD/HOS’s approval is required because of the costs involved in the sending of the fax. The application form for an outbound fax account can be found on the link below:

http://intranet.wits.ac.za/gtd/itsupport/cns/Pages/Fax-to-Email-Application-Form.aspx

SECTION C5 - HARDWARE AND DEVICES

SECTION C5.1 - HARDWARE PURCHASING / PROCUREMENT

The University has certain policies for the procurement of hardware. For desktops, laptops and other mobile devices, there are approved brands and models as well as certain approved vendors from which these can be purchased. The policy can be viewed by clicking on:


For a full list of current approved hardware brands and models, refer to the CNS Intranet, under the "About Our ... "-section.

These would form part of the University Asset list library and would carry a warranty which would include University licensed software.

For quotations or ordering new desktops or laptops email:

#Dept-CNS-ITQuote@wits.ac.za or #Dept-CNS-ITOrder@wits.ac.za or phone 011 717 1603

NB. For Staff and Students who would want to purchase a desktop, laptop or device for personal use, PURCO on behalf of the South African University’s, negotiated prices with specific suppliers for specific laptops that are now being offered to qualifying staff and students. All transactions relating to the procurement of the laptops are between the computer supplier and the end-user. There is no financial gain for the University. PURCO is the Purchasing Consortium of Southern Africa

Click on http://www.stp.ac.za/
Or call 0800 22 37 33 /0800 ACERED
SECTION C5.2 - FAULTY HARDWARE

Under Warranty
CNS will provide assistance in logging a ticket for the repair with the approved vendor, and guiding the user with the faulty hardware through the repair cycle.

Not under Warranty
CNS will provide the contact details for the approved vendors where out-of-warranty support can be procured. This support is for the cost centre of the area that owns the hardware.

END-OF-LIFE HARDWARE SALVAGING
CNS provides a service for end-of-life hardware to assist in disposing of such equipment in an eco-friendly manner. Hardware is collected from the user and an audit performed on the hardware as a part of this service.

SECTION C5.3 - SECURING DESKTOP PCS
In the instance of an office area or computer lab needing to be secured, CNS will secure the desktop or supply the security cabling at cost for staff. For non CNS computer labs, the School or Department would be required to pay for the time of the Student Assistant who would perform the task of securing as well as the cost of the security cabling.

Please send any comments or suggested Changes to this guide to
KIMComms@wits.ac.za

WITS Computing Services For Staff and Students
Version 7.0.0 2015
CNS Service Desk, 1st Floor, West Wing, Senate House Building, East Campus
Tel: 011 717 1717

E-mail: ITStudentHelp@wits.ac.za
CNS – Making IT easy,
Get IT Savvy!
Use this guide

Take the Eek out of Geek!
Do it yourself!