

Connecting to Wi-Fi

Version 2.0



Corporate IT Services

**January 2008
Andrew Leask**

Updated: October 2009
N Daly

Contents

PRE-REQUISITES	3
INTRODUCTION	4
TERMS & CONDITIONS OF USE	5
SECURITY WARNING!	6
CONFIGURATION GUIDE FOR WIRELESS NETWORK	7
CONFIGURING WINDOWS XP (USING THE BUILT-IN CLIENT)	7
CONFIGURING WINDOWS VISTA (USING THE BUILT-IN CLIENT)	11
CONFIGURING MAC OS X (USING THE BUILT-IN CLIENT)	15
WI-FI LOCATIONS ON CAMPUS	19
ACCEPTABLE USE POLICY	21
FOR MORE HELP	22
USEFUL LINKS	22

Pre-requisites

- Agreement with the College *Acceptable Use Policy* (see page 21)
- Any personal Wi-Fi equipment compatible with IEEE 802.11a, b, or g
- A valid logon to the Aspire Domain
- You must have logged onto a wired connection at Doncaster College before the wireless connection will connect to the Internet. This is because your username and password has to be *initially* authenticated over a wired connection.

Introduction

Wireless LAN (a.k.a. *WLAN* or *Wi-Fi*) access to the Internet is available for students, staff and registered guests using their own equipment from a number of Wi-Fi enabled areas on Campus.

This connection is via the Academic service provider JANET and therefore users are expected to abide by both the local Doncaster College and the national JANET network *Acceptable Use Policies*. The use of wireless provision in open access areas (such as the LRC) is further subject to any local policies or rules.

This service is provided to users with no guarantees, may not be shared or transferred to anyone else and may be rescinded at the Colleges discretion at any time. Use of this access will be deemed an acceptance of the following terms and conditions.

Terms & Conditions of Use

1. Use of this IT facility is subject to the Doncaster College *Acceptable Use Policy* as detailed below and failure to adhere to this policy will result in withdrawal of this facility and may involve legal action as appropriate.
2. Doncaster College will not be held responsible or liable for damage to data or any resulting loss of earnings suffered by users of the service as a result of malicious computer use by other local network or Internet users. This covers, but is not limited to; *viruses, worms, trojans, spam, spyware, malware* and any other “*hacking*”, “*cracking*” or *denial of service attacks*.
3. Internet access bandwidth is provided as available to the College through its JANET connection *in contention* with its other networks for College staff and students. We make no promise or guarantee that there will be sufficient data rate (i.e. Megabits per second) available for whatever services that users choose to use.
4. For the purposes of supplying evidence to law enforcement in the event of an incident Doncaster College Corporate IT Services reserve the right to log network access requests by users of this network and to undertake any network scans, probes or investigations as deemed necessary to protect the security and reputation of Doncaster College in the Academic Internet community.
5. If you encounter connection problems please contact the CITS Service Desk as detailed below. We will do our best to help you.

Visitors welcome

**CITS Helpdesk
N.3.606
The Hub
Doncaster College
Chappell Drive
Doncaster
DN1 2RF
Tel: +44(0)1302 553646
Fax: +44(0)1302 553568
Email: help.desk@don.ac.uk**



Opening Hours: 9am to 5pm (Mon-Thurs) & 9am to 4.30pm on Fridays

Out of hours by prior arrangement.



Security Warning!

Use of your equipment on this shared, Internet facing network is at your own risk and we **strongly** recommend that you install your own protective measures.

We also recommend that you make sure that the updates on your operating system and protective tools are up to date.

As a general rule of thumb:

You should avoid doing any banking or shopping via a public hotspot, period!

There are 12 Doncaster College Wireless Hotspots (Resnet) installed at various locations throughout The Hub.

Please see the 3D maps available on the Student & Staff intranets for exact locations of all these Hotspots.

There are 21 Doncaster College Wireless Hotspots (Resnet) located around the High Melton site.

The 3D Map for High Melton will be arriving soon.

Configuration Guide for Wireless Network

1. Please make a note of any of your existing settings so that they can be returned after leaving the College.
2. If you are an experienced Wi-Fi user or have a proprietary wireless client you can shortcut the rest of this guide and just use the settings below.

- **IP Address** – set to DHCP
- **SSID** – Resnet (*Note the capital R*)
- **128 Bit WEP Key** – 1010101010101010deadfeed
(*this is basically 9 x “10” characters followed by deadfeed*)
- **Internet Proxy** 10.2.3.33 Port 8080

3. If you need more help and are using the standard built-in client for accessing WLAN networks that comes with Windows XP, Windows Vista or Mac OS X use the instructions below.

There are 3 basic steps to configure your computer for access to the College Hotspots. Each distinct step in this guide will be preceded by the step number. You don't necessarily have to follow the step order, but you **MUST** complete all 3 steps to connect to the Internet.



1. Configure the computer to get an IP address automatically using DHCP.



2. Go to an area within range of a hotspot and connect to the Hotspot using the “Network Key” or “Password”.



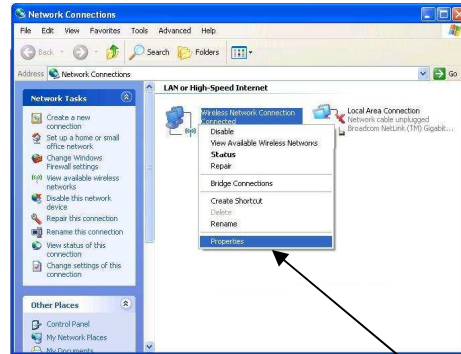
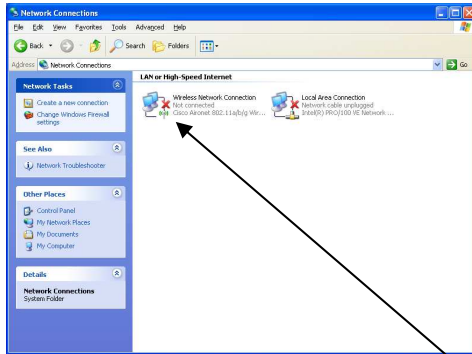
3. Configure your browser to connect to the Internet using a proxy server to authenticate your identity.

The following pages will provide details of how to accomplish each of the three steps above.

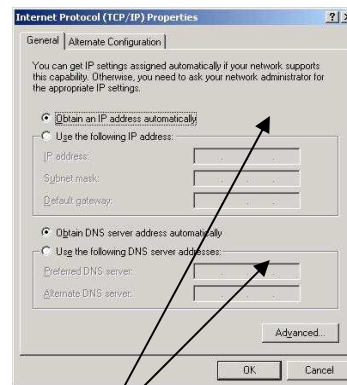
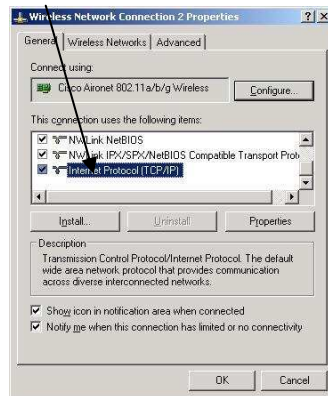
Configuring Windows XP (using the built-in Client)

1

1. Go to "Start".
2. Click on "Control Panel".
3. Click on "Network Connections".



4. Right click on the "Wireless Network Connection" and pick "Properties".
5. Double click "Internet Protocol (TCP/IP)" or highlight and click "Properties".

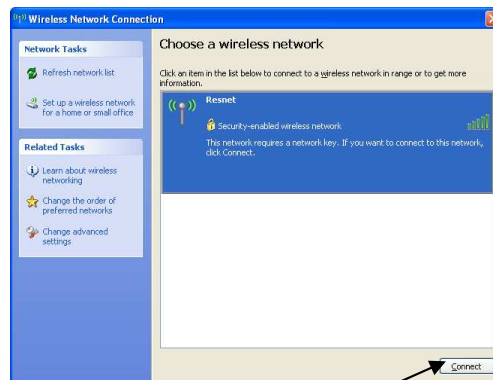
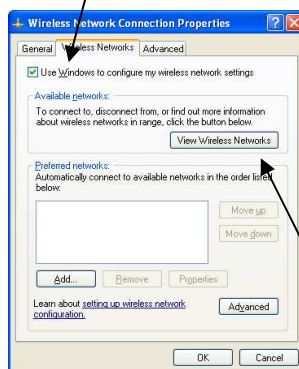


6. If there are any IP addresses already in here then please make a note of them before moving onto the next step, (you may need them for your home network).
7. Pick "Obtain an IP address automatically" and "Obtain DNS server address automatically".
8. Click "OK".

Click on "Wireless Networks"

2

1. Ensure that the "Use Windows to configure my wireless network settings" is ticked.

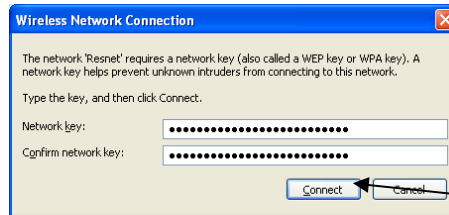


Resnet is Doncaster College's wireless network.

2. Click on "View Wireless Networks"
3. Highlight "Resnet" and click on "Connect".



You will see the following screen as your computer attempts to connect to the Wireless Access Point.



Once you are connected you will be asked for the “Network Key”.

4. Type the “Network key” as “1010101010101010deadfeed (9 x “10” characters)” into the “Network key” box,

AND ALSO into the “Confirm network key” box.

5. Click “Connect”.

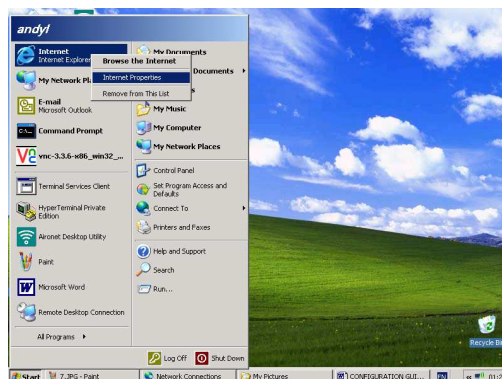
This will only have to be carried out once.

Once you have successfully connected to Resnet, you will automatically connect to Resnet whenever you are in range of a Doncaster College Wireless Hotspot.



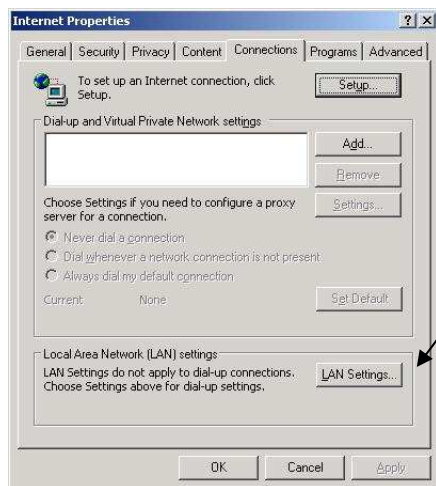
Setting the Internet Explorer Proxy

1. Right click on the Internet Explorer icon in your Start Menu as shown and pick *Internet Properties*.

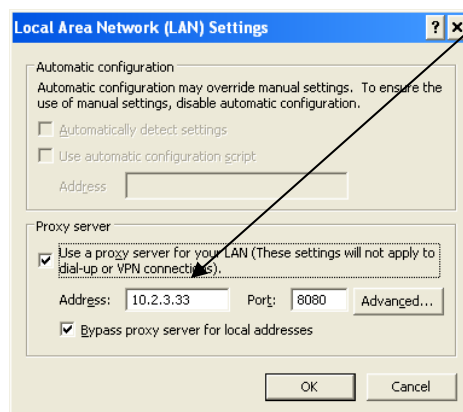


Note: This can also be chosen by opening Internet Explorer and picking *Internet Options* from the *Tools* menu.

2. Pick the Connections tab and then LAN Settings



3. Please tick “Use a proxy server for your LAN....” and type “10.2.3.33” in the Address box, and “8080” in the Port box as below.



4. Click “OK” twice to close the dialog boxes.

The configuration is now complete.

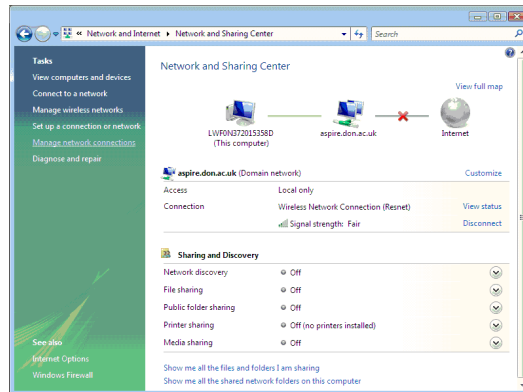
When you try to use the Internet you will be prompted to enter your username and password.

NOTE: You must have logged onto a wired connection at Doncaster College before the wireless connection will connect to the Internet. This is because your username and password has to be *initially* authenticated over a wired connection.

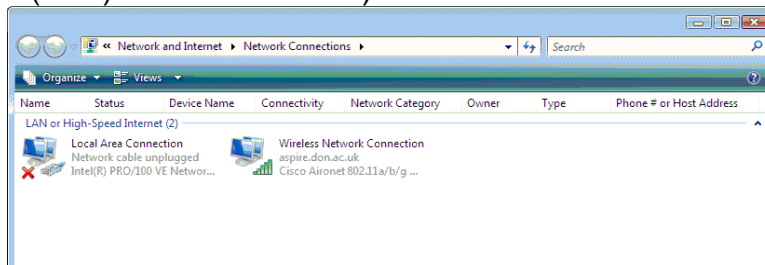
Configuring Windows Vista (using the built-in Client)

1

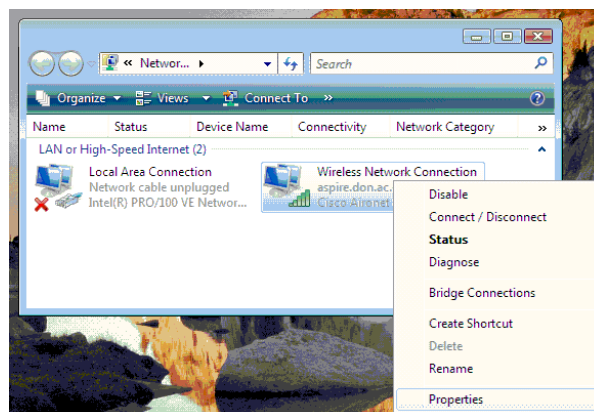
1. Setting up your wireless network card to get IP address and DNS information automatically.
 - a. Click on the Windows Start button and then Click on “Control Panel”.
 - b. In the Control Panel, under the “Network and Internet” section, left-click on the link "View network status and tasks".
 - c. **Note:** If your computer's Control Panel is setup to show Classic View, this is called "Network and Sharing Center" which must be double-clicked.

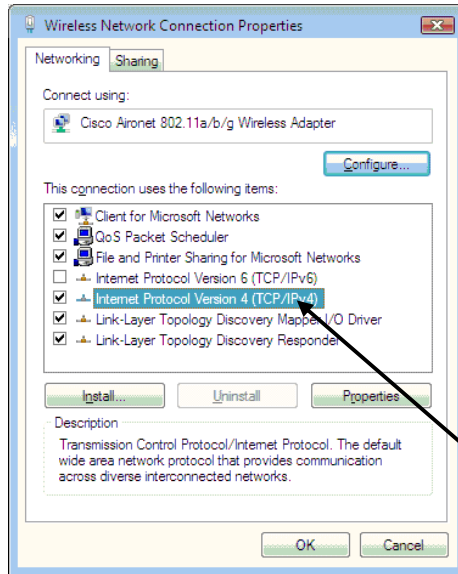


- d. Once in the “Network and Sharing Center” click on the link in the left-side list entitled "Manage network connections".
 - e. This opens a new window which should show the network adaptors in your machine (as you can see I have two - one wired (LAN) and one wireless).

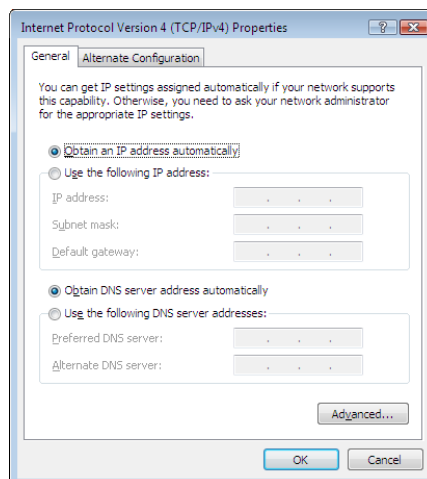


- f. Use the right mouse button to click on the icon describing your wireless connection - it will open a contextual menu as shown below... Choose the “Properties” option.



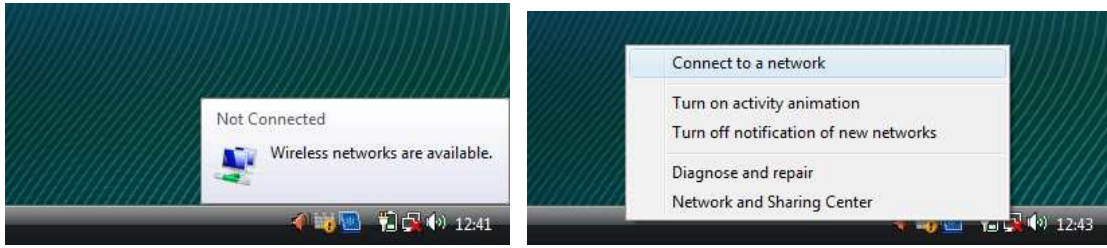


- g. Select and highlight “Internet Protocols Version 4 (TCP/IPv4)”.
- h. Click the “Properties” button.
- i. Properties for this need to be set to get an IP address and DNS info automatically as shown below.

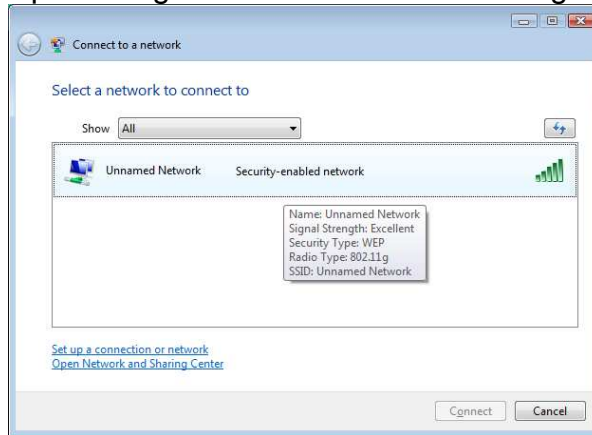


Connecting to a Wireless Hotspot

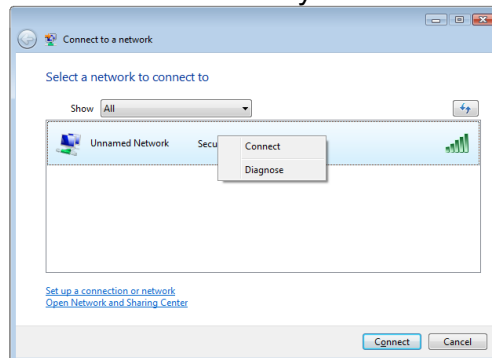
1. Now take your computer to a location covered by the College wireless service and switch on. The SSID is broadcast as “Resnet”.
2. Hovering your mouse pointer over the network tray icon (the one showing two screens with a red “x” as shown below) shows that wireless networks are available.



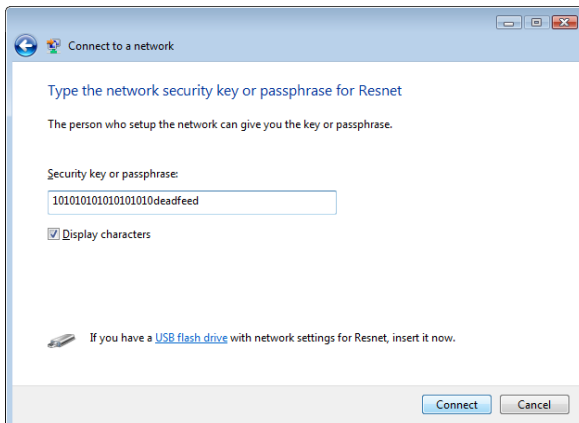
3. Right click on the icon and choose the “Connect to a network” option.
4. This brings up a dialogue as shown below showing available networks.



5. Highlight the “Resnet Network” entry and click on “Connect”.

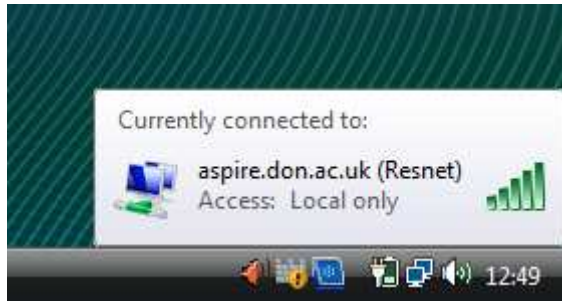


6. Enter the Security key when prompted. As mentioned above this is – **1010101010101010deadfeed**



7. Click on “Connect”.

7. If you have entered the Security key correctly the connection should now be established.
8. Click “Close” and the settings will be saved.



Setup your Proxy server settings for your Internet browser as detailed in the [Windows XP instructions](#) above (page 9).

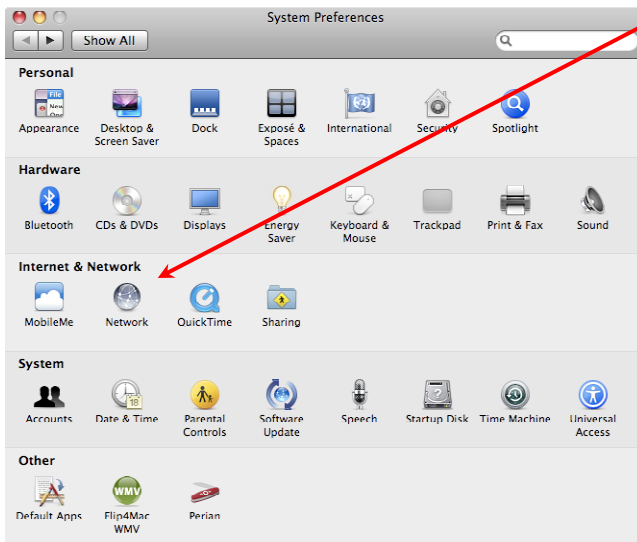
NOTE: You must have logged onto a wired connection at Doncaster College before the wireless connection will connect to the Internet. This is because your username and password has to be *initially* authenticated over a wired connection.

Configuring Mac OS X (using the built-in Client)

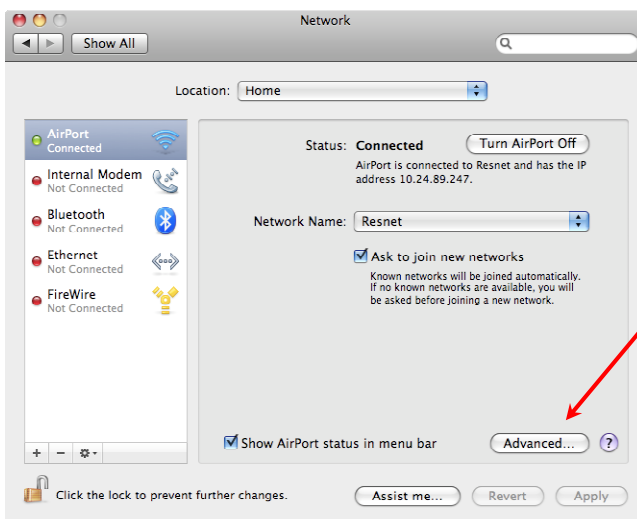
1

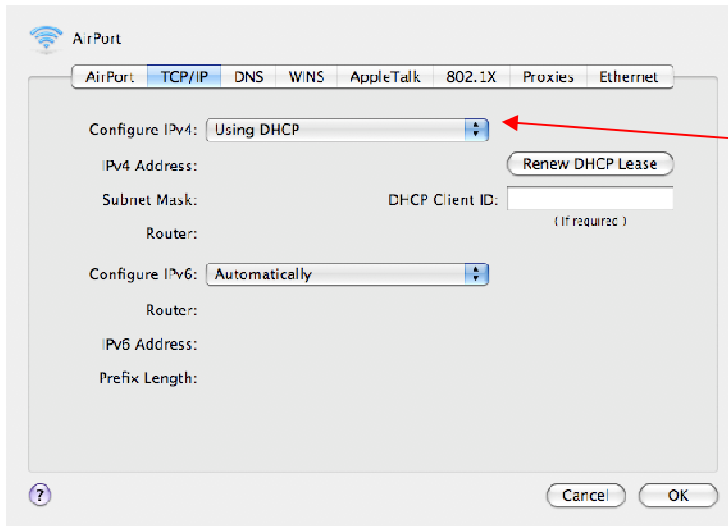
1. Setting up your wireless network card to get IP address and DNS information automatically.

Call up the System Preferences... Go to the "Network" preferences...



Highlight "AirPort" and click on "Advanced"





Make sure that "Configure IPv4" is set to "Using DHCP".

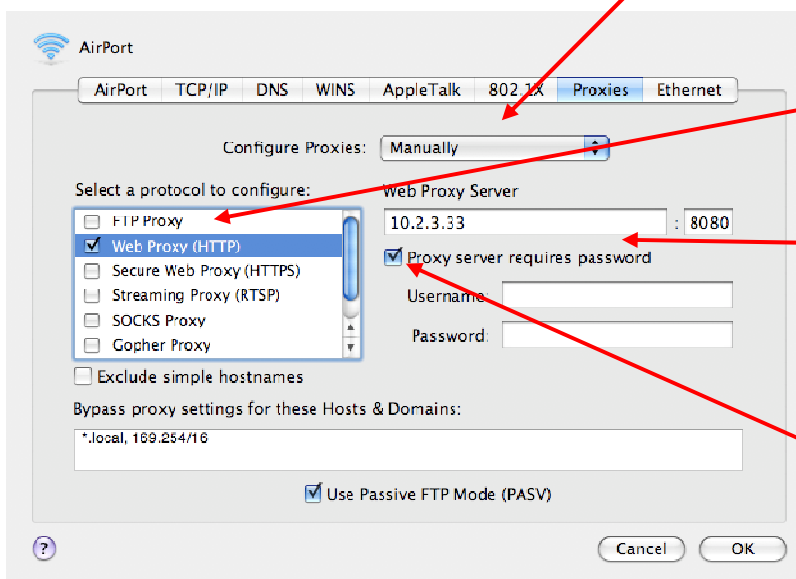
3

Setting the Proxy Server Settings

While we are in Network Preferences we can also complete Step 3.

Click on the "Proxies" tab.

Choose "Configure Proxies" as Manually



Highlight "Web Proxy (HTTP)" and tick the box.

Enter the "Web Proxy Server" address as 10.2.3.33 : 8080 as in the screenshot.

Tick the box, "Proxy server requires a password".

Click OK

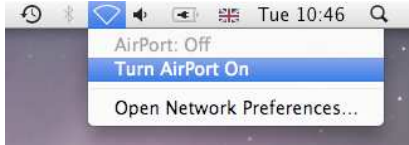
Click Apply

Close Network Preferences

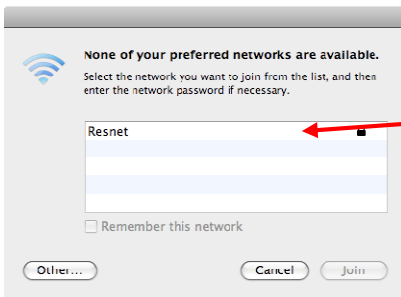


Connecting to a Wireless Hotspot

Go to a location covered by the College wireless service and ensure that AirPort is switched on.

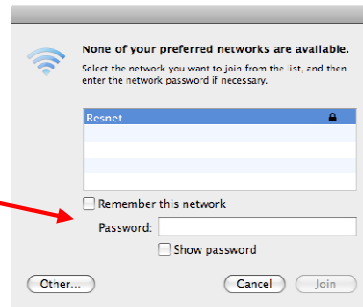


The SSID is broadcast as “Resnet”, and you should see the following screen.



Click on “Resnet”

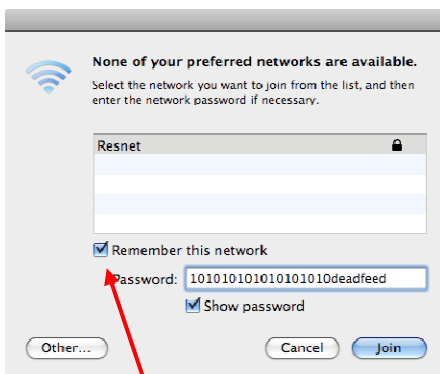
Further options will appear



Enter the password as:

101010101010101010deadfeed

Which is basically 9 sets of “10”, followed by dead feed.



Click on “Remember this network”. This will allow you to connect automatically to all Resnet Hotspots situated around the College.

Click “Join”

Open your browser.

If your computer is configured correctly you will be prompted for a user name and password when you attempt to connect to the Internet.



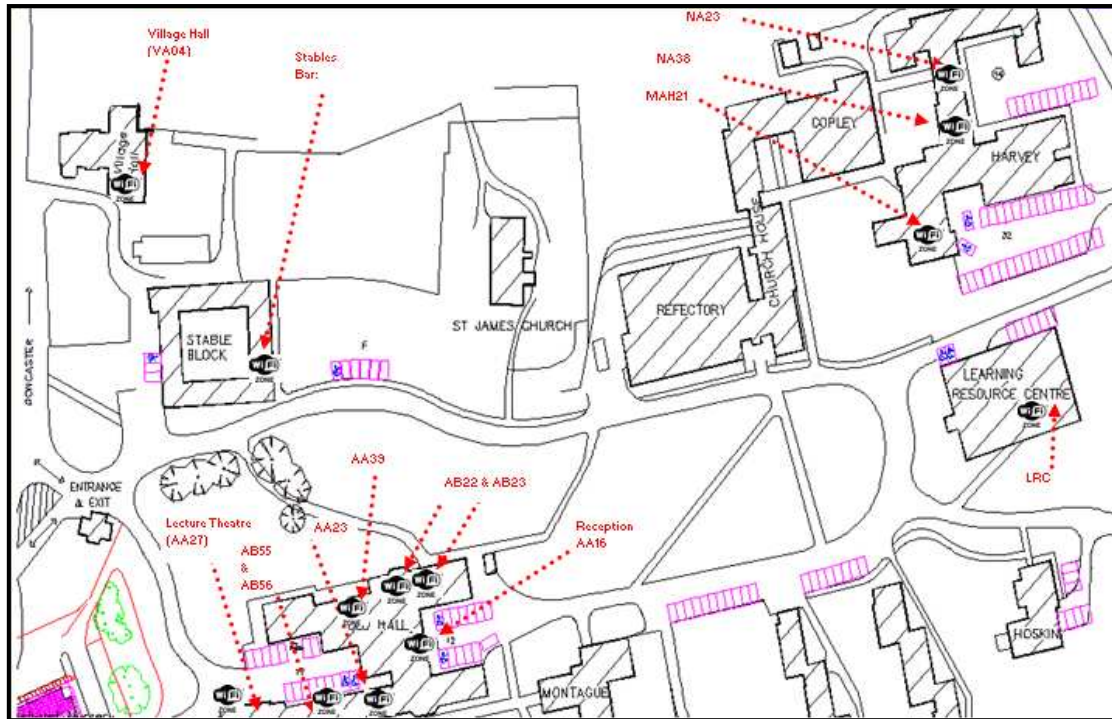
Please enter your "DC Number" if you are a student, followed by @don.ac.uk.

If you are a member of staff then your username will be "*firstname.lastname*", followed by @don.ac.uk.

NOTE: You must have logged onto a wired connection at Doncaster College before the wireless connection will connect to the Internet. This is because your username and password has to be *initially* authenticated over a wired connection.

Wi-Fi Locations

High Melton Campus



LRC (Main Ground Floor Area)
Refectory (Bar Area & Eating Area)
Stables (Blair Athol Bar Area)
Pavilion (Bar Area)

Copley (QA11, QB13, QB16)
Church House (RB12, RB15)
Harvey (NB09, MAH21-Drama Hall, MAH26-Dance Studio)
Montagu (MC40)
Old Hall (AA23, AA27, AA39, AB22, AB23, AB56)
Hoskins (HA02 – Common Room)

Note: This map is only to give an indication of the coverage and does not constitute an agreed service level. The true coverage will depend on the wireless card used.

The Hub

South Block

LRC (Levels 3 and 4)
S.1.930 Front of House/Learner Services (coverage extends to ground floor Coffee Bar Area)

North Block

N.2.602 Coverage extends to multiple locations, including:

- Central Atrium between North and South Blocks
- Top of Atrium escalators outside Level 2 lifts
- Motor Vehicle Workshops – North Block Level 1
- Events Hall – North Block Level 1
- Refectory – North Block Level 1

N.2.612U Coverage extends outside to grassy area near river entrance
N.3.620 Conference Room (coverage extends to some surrounding areas)
N.4.702 Coverage for Drama Theatre
N.5.628

East Block

E.2.104 Engineering
E.3.120 Engineering
E.4.176 Childcare 1
E.4.204 Childcare 2

The Hub coverage is also available as a 3D map on the College Intranet.

Acceptable Use Policy

The following regulations apply to users of all IT facilities owned, leased or hired by the College, all users of IT facilities on the College's premises and all users of IT facilities connected to the College's networks. Users must also comply with any further specific instructions or regulations displayed alongside computing facilities or on computer screens.

- 1.** Use of the IT facilities is subject to the provisions of the Data Protection Act 1998, the Copyright, Designs and Patents Act 1988 (and subsequent regulations), the Computer Misuse Act 1990, Data Protection Act 1998, Anti-Terrorism Crime and Security Act 2001, Regulation of Investigatory Powers Act 2000, Freedom of Information Act 2000, Companies Bill, Civil Contingencies Bill and the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.
- 2.** IT facilities are made available, for bona fide educational use, to staff and enrolled students of the College. Other persons may also be authorised to use facilities, by the Director of IT for centrally-provided facilities, or the head of any other relevant unit of the College responsible for a particular facility.
- 3.** Users must not cause any form of damage to the College's computing equipment or software, nor to any of the rooms and their facilities and services which contain that equipment or software. The term "damage" includes modifications to hardware or software which, whilst not permanently harming the hardware or software, incurs time and/or cost in restoring the system to its original state. Costs associated with repairing or replacing damaged equipment or software and/or in providing temporary replacements may be charged to the person or persons causing the damage. The costs will be determined by the designated authority.
- 4.** Use of certain facilities requires prior registration and the granting of a user code and/or an individual password. The granting of a user code and password will constitute authorisation for use of relevant facilities for the term agreed only. Users must not use another user's code, nor permit or allow another user to use his/her own code. Users must not allow any password associated with his/her code to become known to another user.
- 5.** Users must not deliberately introduce any virus, worm, trojan horse or any other harmful or "nuisance" program or file onto any system or take deliberate action to circumvent any precautions taken by the College to safeguard the security of its computer systems.
- 6.** Users must not connect any device into the College's network without prior agreement from the appropriate designated authority. Guest (i.e non-staff or non-student) users, who if by prior agreement are granted access permissions, must only use those network points, areas and facilities for which permission has been agreed.
- 7.** Users must not make use of any of the College's computing equipment to connect to any other computing facilities or commercial services without prior permission and appropriate registration.
- 8.** Users of networking facilities must follow any rules published for use of the networks and/or any computer systems to which he/she has access over those networks.
- 9.** The use of any of the College's computing facilities for commercial gain, for work on behalf of others or for private or personal use (unconnected with a student's course of study at the College or a member of staff's legitimate activities) is not allowed unless prior agreement has been made with the designated authority for the facilities and an appropriate charge for that use has been determined.
- 10.** Certain facilities may be chargeable. Failure to pay outstanding charges may result in withdrawal of services and/or withholding of awards.
- 11.** Interfering with, or disrupting in any way, the computing services and facilities available to other users, is not allowed.
- 12.** Smoking, eating or drinking in any student workstation or PC room is not allowed.
- 13.** Computing facilities provided by the College must not be used to produce, obtain, store, display or distribute material of an obscene, pornographic, offensive or abusive nature.
- 14.** Computing facilities provided by the College must not be used to abuse or harass anyone, whether or not they are members of the College.
- 15.** The College reserves the right to monitor usage of its computing facilities, in order to ensure their proper use according to the above regulations. Such monitoring may be undertaken randomly.
- 16.** Failure to observe any of these regulations may result in withdrawal of access to IT facilities, local, College-wide or external, at the discretion of the Head(s) of the Department(s) concerned. It may also result in a recommendation that the infringement be pursued via the College's formal disciplinary procedures. Infringement of certain regulations may be subject to penalties under civil or criminal law and such law may be invoked by the College.

For More Help

If you need more help please call the IT Helpdesk on x3579 or via help.desk@don.ac.uk.

Useful Links

Further reading - Wireless Networks explained

<http://reviews.zdnet.co.uk/hardware/networking/0,39023970,10002769,00.htm>

Further reading - Securing your Wireless Network

http://www.practicallynetworked.com/support/wireless_secure.htm

LastEditor: Noel Daly, 22/10/2009