TAFE SA STUDENT WIRELESS ACCESS

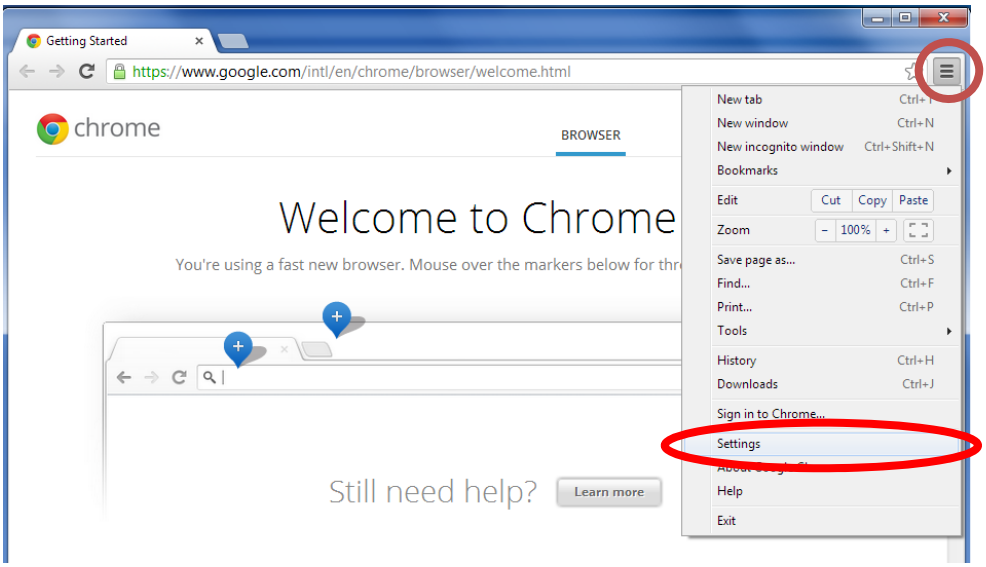
GOOGLE CHROME

PERFORM THE FOLLOWING STEPS TO ACCESS THE INTERNET USING THE TAFESA-INTERNET WIRELESS SERVICE

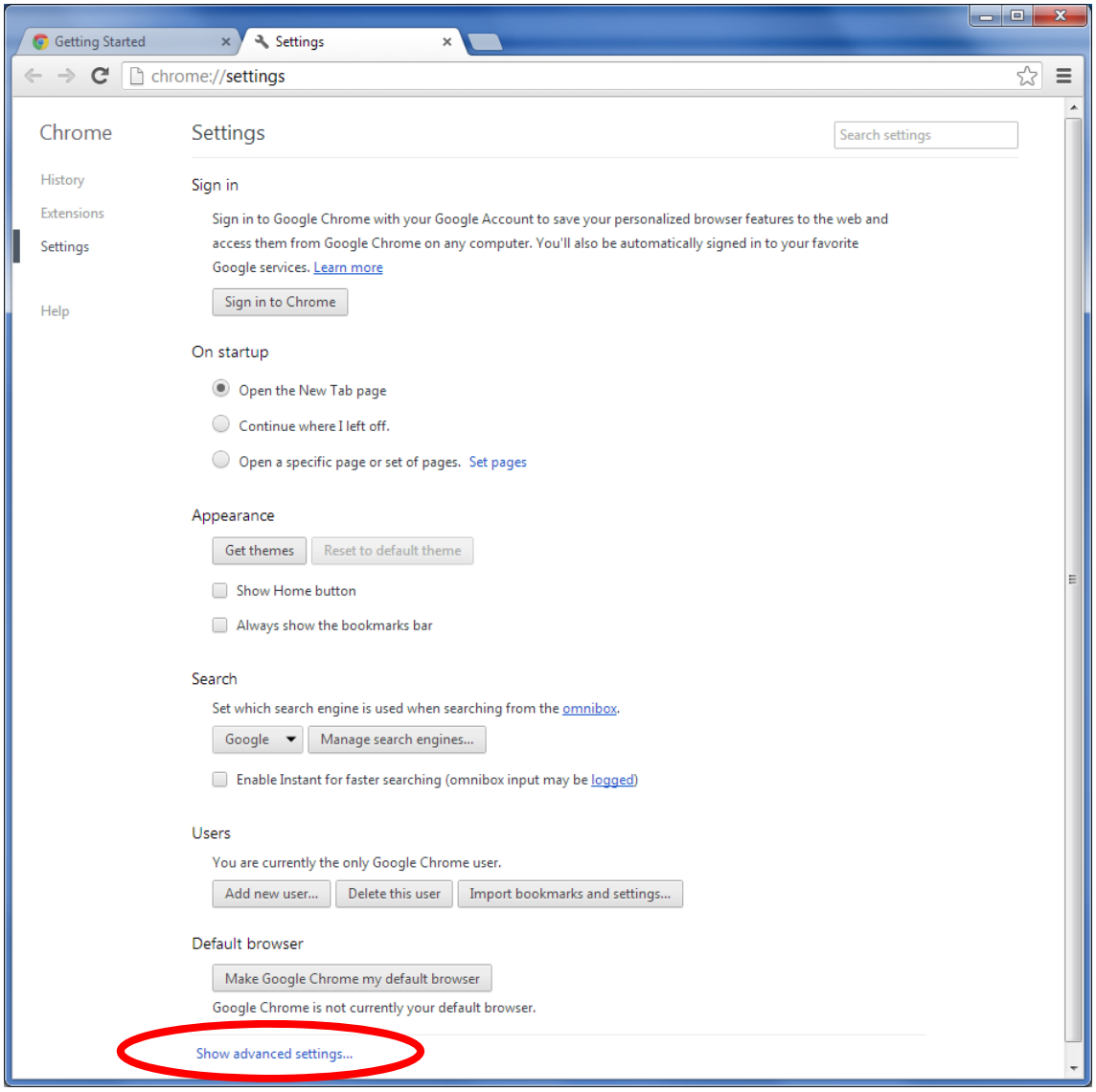
1. Using your wireless adapter software, browse for and connect to TAFESA-Internet. If you encounter issues please refer to the corresponding TAFE SA wireless network guide for your operating system located at http://www.tafesa.edu.au/services/student-wireless-network.

2. Configure the browser to use a proxy server as illustrated below.

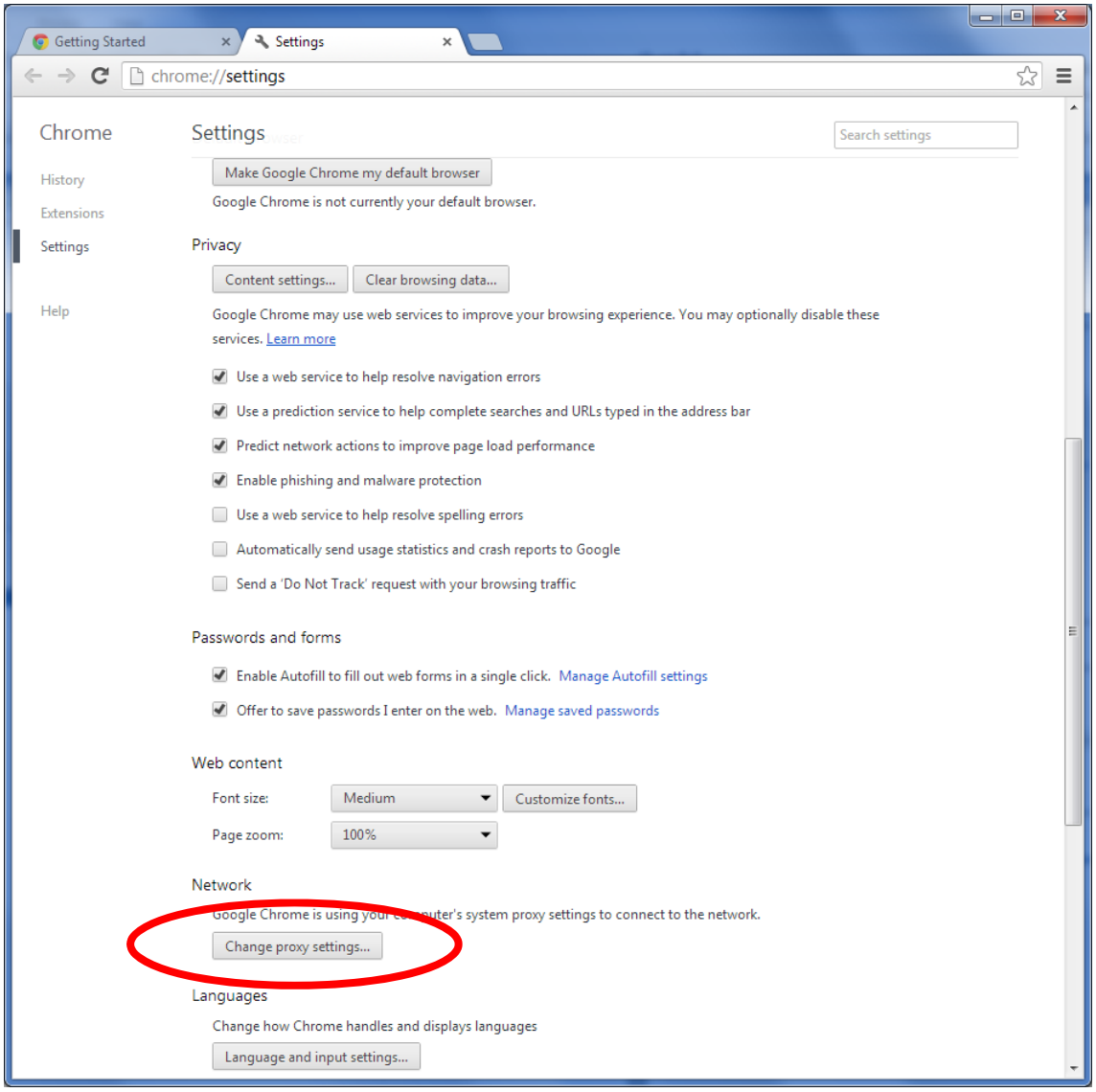
   - Click on the ***Page*** icon on the taskbar and select ***Settings***.



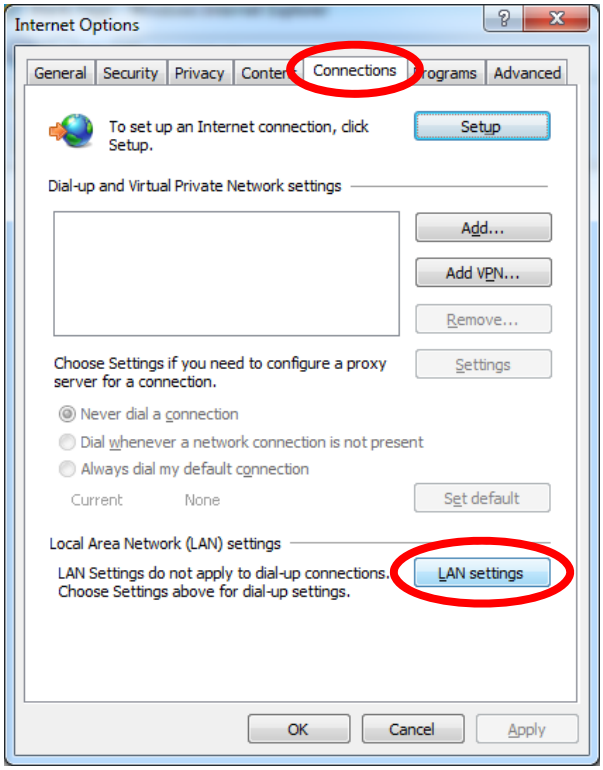
- Scroll down and click on ***Show Advanced Settings…***.



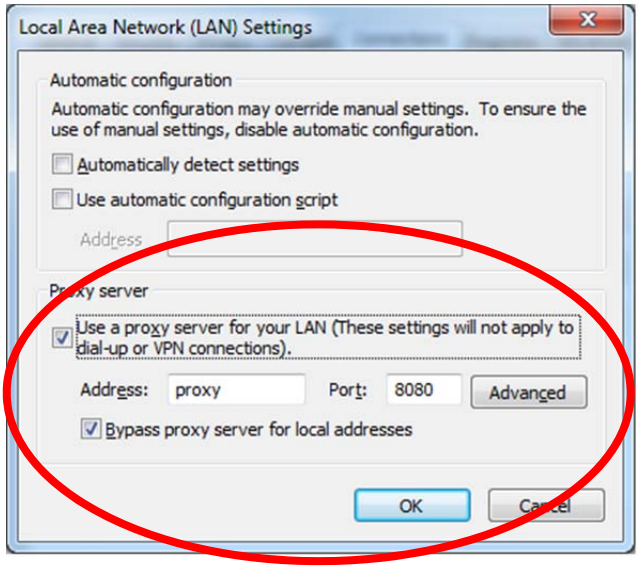
- Scroll down and click on ***Change proxy settings…***.



- In the ***connections*** tab, select ***LAN settings***

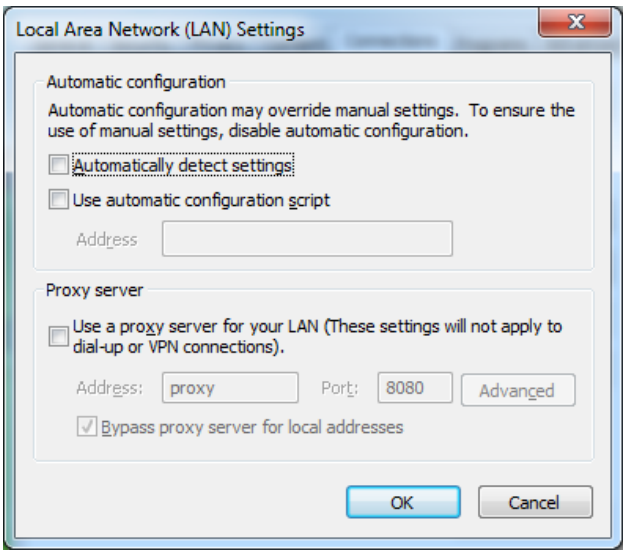


- Ensure ***Use a proxy server for you LAN*** and ***Bypass proxy server for local addresses*** is ticked, leaving everything else un-ticked. In the ***Address*** field enter **proxy** and in the ***Port*** field enter **8080**. Select ***OK*** and ***OK*** again.



3. After these steps are done correctly you should be able to browse the internet.

4. When you are finished browsing remember to reverse changes in step 2, removing any proxy settings that may prevent internet access when at home or on other networks.



Disclaimer: *The Department of Further Education, Employment, Science and Technology (DFEEST) is not liable for any loss resulting from any action taken or reliance made by students on any information contained within this document (including, without limitation, third party information). Students obtain access to the wireless network at their own risk and DFEEST accepts no responsibility for any interference, loss, damage or disruption to privately own computer system which arises in connection with the use of this network. Students must take their own precautions to ensure that the process which they employ to obtain access to this wireless network does not expose them to the risk of viruses, malicious computer code or other forms of interference which may damage their own computer system.*