AUP: Wireless Acceptable User Policy

Purpose

This document addresses the risk of using the wireless systems, the policies required to manage those risks to an acceptable level and the responsibilities within the college to achieve this

Acceptable Use Policy for the Wireless Network

Misuse of your college Wi-Fi network connection will lead to the withdrawal of your wireless connection privileges, and for staff and students of the college, may have consequences for other forms of access to the College's network resources

Rose Bruford College provides this wireless networking on the basis of 'as is' principally for the use of staff and students, to help achieve the college's and the students' educational objectives. The network design is such that commercial and academic traffic is securely partitioned from each other

The College applies a Network Access Protection (NAP) policy to wireless clients during initial authentication that require all clients to have the firewall enabled on all network connections, and on Windows clients to have anti-virus and malware software installed, running and up to date. This is to ensure that other clients on the wireless network are protected. Failure to meet the NAP policy fully will possibly result in denial to the wireless networks.

Some wireless network SSID's will allow only one authentication per staff/student login and will automatically timeout after a specific time frame, this is to manage load sharing and licensing

The College supports personal (non-academic related) use of the wireless network service, to develop skills related to the performing arts industry. However, some restrictions must be imposed in the ways in which the network may be used

General Restrictions

Your usage of this network is regulated by relevant UK law, and it is your responsibility to familiarise yourself with its requirements. (see for example Data Protection Act 1998; Parts of the Criminal Justice and Public Order Act 1994; Computer Misuse Act 1990; Copyright, etc. and Trade Marks (Offences and Enforcement) Act 2002).
In particular, you MUST NOT use the network to:

- Access, send or otherwise make available to others any material that is offensive, obscene or indecent, or infringes the copyright of another person (for example, MP3 or other audio or video formats). The United Kingdom has strict laws on obscenity. You should also be aware that copyright law still applies to the Internet.
- Do not make available by any means (web server, FTP server or file-sharing (P2P) software such as KaZaa, Gnutella, Morpheus, etc.) any material unless you are the copyright holder of that material, or have a licence to make that material available, or the material has been expressly put into the public domain and you can demonstrate this. By material we mean any information that can be stored on a computer: multi-media files such as video, music, speech, etc.; still images; text; software; or other file formats. An explanation of copyright is available on the UK Patent Office web site; global copyright is explained at the World Intellectual Property Organisation site.
- Cause annoyance, inconvenience or anxiety to others. Examples would include abusive or offensive Emails.
- Access or attempt to gain access to, computer systems, data or resources to which you are not authorised. Only use those resources that you have permission to access.
- Provide network services (such as DNS, DHCP, BootP or other such services that may interfere with the normal running of the network). Rose Bruford College provides such services. You should make sure that your PC does not. In general, this applies more to students running versions of Unix, such as Linux and OSX, but versions of Windows can also sometimes provide some of these services.
- Provide access to other users (for example by connecting a hub or modem to a Wi-Fi networked PC, or by passing on your username and password to a third party).
- Access network services in such a way as to deny reasonable access to the network for other users, for example, by excessive use of network bandwidth. This could include the use of personal web or FTP servers, or file-sharing software

The college provides each user with a unique IP address for the duration of their wireless network session. You should never change your IP address settings

Restrictions specific to staff and students of the College

Network traffic for members of the college is routed over the campus network and out to the Internet via the publicly-funded JANET network or commercial solutions like BT and BSkyB. Some additional conditions and responsibilities fall upon its users. Your use of the network must abide by:

- College policies, including 'Standards and Guidelines for all Users of College Computing and Network Facilities', Internet AUP and Student Policy on Social Networking Websites
- the acceptable use guidelines of JANET - SSID eduroam
- the acceptable use guidelines of 'The Cloud' - SSID The Cloud
- the acceptable use guidelines of BT OpenWorld - SSID RBC-INTERNET

Records & Monitoring

Note that everything that is done using the campus Wi-Fi network is automatically recorded and stored. These records (of web sites visited, files transferred, emails sent, etc.) are not actively monitored, but if any misuse is suspected, they may be checked (in accordance with College, BSkyB or BT regulations respectively) to find out exactly what any user was using the network for at any given time. If you keep within the acceptable use guidelines specified above, your records will never be looked at

Misuse of the network facilities including, but not limited to, those listed above will regarded as a serious disciplinary matter within the College. Misuse will result in the immediate termination of your network access. It may also result in disciplinary action being taken by the college authorities or even the UK police.

IT staff oversee and monitor your usage of network facilities. Under exceptional circumstances, and with permission from the Principal, IT personnel may be authorised to inspect a particular computer on site (including the data and services running on it). In such cases, the registered user will be required to co-operate with the inspection (for example, by providing any passwords required)

You should also be aware of the possible security risks associated with connecting your computer to a network. It is your own responsibility to keep your computer free from malicious code (i.e. viruses, etc.) and secure it against unauthorised access (i.e. 'hackers'). You are strongly advised to take precautions such as installing up-to-date anti-virus software and applying any security 'patches' issued by your operating system provider