Residence Network Acceptable Use Policy

INTRODUCTION

Mount Royal University (MRU) Residence Services provides guests with high speed Internet connection. The purpose of this connection is to enhance and support the educational experience of the guest by facilitating the sharing of knowledge and information. We encourage all guests to be responsible at all times when using the network services in Residence. This is for the well-being of everyone and to provide equal high speed access opportunities for all guests in Residence.

The use of Internet access must be in compliance with this policy, the MRU Residence Conduct Guide (http://www.mtroyal.ca/residence/) and the Code of Student Conduct policy of MRU (http://www.mtroyal.ca/codeofstudentconduct/). MRU reserves the right to restrict access to inappropriate web sites, inappropriate web resources or inappropriate network traffic.

Failure to comply with these policies will result in immediate termination of the Internet service. The Internet service may be reinstated upon review by MRU Residence Services and MRU IT Services.

For the purpose of this policy:

- ResNET is defined as both the wired and wireless network provided by MRU Residence Services.
- Any Network Devices that are IP network-enabled which connect to ResNET, including but not limited to desktop computers, laptop computers, gaming consoles (XBOX, PS3, Wii, etc), Personal Assistant Devices (PDAs) and Smartphones are covered by this policy.
- A student resident, resident advisor or conference/hotel client who has been granted access to connect and operate a Network Device on the ResNET is covered by this policy. (Reminder: residents and conference/hotel clients are solely responsible for the actions of their guests).

POLICIES

I. ILLEGAL ACTIVITY

Use of the ResNET for any activity that violates local, provincial, federal or international laws, orders or regulations, is a violation of this policy. Prohibited activities include, but are not limited to:

a. posting or disseminating unlawful material (child pornography or obscene material),

b. disseminating material which violates copyright or intellectual property rights. The customer assumes all risk regarding whether material is in the public domain,

c. pyramid or other illegal soliciting schemes,

d. fraudulent activities; including but not limited to: impersonating any person or entity, or forging anyone's digital or manual signature,

e. accessing illegally or without authorization computers, accounts, or networks belonging to another party, or attempting to penetrate security measures of another individual's system (often known as "hacking"); also, any activity that might be used as a precursor to an attempted system penetration (i.e. port scan, stealth scan, or other information gathering activities),

f. unauthorized use of user names, passwords, computer addresses/identities or modification of assigned network settings to gain access to computer resources and/or data, or otherwise attempting to evade, disable or "crack" security provisions of computer system(s),

g. inspecting, altering, deleting, publishing or otherwise tampering with files or file structures that the individual is not authorized to access,

h. distributing information regarding the creation of and sending Internet viruses, worms, Trojan horses, pinging, flooding, mail bombing, or denial of service attacks. Also, activities that disrupt the use of or interfere with the ability of others to effectively use the network or any connected network, system, service, or equipment.

II. COMMERCIAL USE

ResNET usage for commercial purposes is strictly prohibited. Examples of the breach of this policy are:

a. ResNET to conduct a personal business enterprise.

b. ResNET for profit

c. ResNET for the purpose of advertising

Users may not resell, share or otherwise distribute the internet service or any portion thereof to any third party. For example, you cannot provide internet access to others through a dial up or wireless connection, host shell accounts over the internet, provide email or news service or send a news feed.

III. INTERFERENCE

Users' ResNET usage must not interfere with other users' ResNET usage ability. Additionally, users' ResNET usage must not interfere with the functionality of the remainder of the residence network infrastructure. Interference can be constituted by, but not limited to, the following:

a. Any activity or process that causes another user to be deprived of services or resources that they would normally expect to have available. This includes but is not limited to the creation of "spam" (excessive email distribution) and the introduction of viruses or electronic chain letters into the network environment.

b. Connecting or installing servers onto the ResNET, including but not limited to:

   i. FTP servers

   ii. World Wide Web servers

   iii. streaming media servers

   iv. mail or News servers

   v. DNS servers

   vi. DHCP servers

c. Connecting wireless routers and/or access points to ResNET.

d. The creation of a Wireless Local Area Network (WLAN)

IV. LIABILITY

As a user of the ResNET, you accept full responsibility for all activity that is associated with your network connection.

V. BEST PRACTICES

It is recommended that all users follow best practices in maintaining their computer's security and stability to ensure that their ResNET connection is not misused. Such best practices include, but are not limited to:

a. Turn your computer on only when you're going to use it.

b. Lock your bedroom or lock your computer to avoid inappropriate use by guests

c. Supervise your guests when using your computer and ResNET services
d. Do not open suspicious e-mail, especially if it includes an attachment.
e. Install all current security patches to your Operating System.
f. Install and use AntiVirus software with current virus definitions.
g. Be discerning about what software you download and install on your computer. Many downloads are SpyWare.
h. Make use of a Spyware removal tool like Spybot Search and Destroy or AdAware.
i. Make use of personal firewall software like Norton Personal Firewall or ZoneAlarm.
j. Be cautious when sharing files with others. They may not be as careful as you are!
k. Turn off unneeded network-connected programs or services.

VI. VIOLATION OF ACCEPTABLE USE POLICY

In the event that a computer user violates this policy, they shall be subject to disciplinary action, including

a. immediate termination of their ResNET connection
b. a direction that such misuse cease and desist,
c. the possibility that the user reimburse MRU or pay for computer and network resources,
d. denying the user access to computer and network resource(s) temporarily or permanently, and/or
e. appropriate MRU disciplinary sanctions as described in the Residence Conduct Guide and/or the MRU Code of Student Conduct

VII. REPORTING ABUSE

You are encouraged to report an abuse of this policy to the ResNET office in RB1011. Your report will be kept confidential. It would be helpful to include copies of any document or communication that is relevant as well as dates and times of the occurrence, etc.

VIII. QUESTIONS

If you have any questions related to acceptable use of the Mount Royal University ResNET or require technical support, please contact the ResNET help desk at 403.440.8888, via e-mail at res-tsa@mtroyal.ca or the ResNET office in RB1011.