

Policy Title	ResNet Acceptable Use Policy
Policy Statement	All Towson University (TU) students connecting to the Residential Network (ResNet) must comply with acceptable uses of the network in order to ensure a stable and safe computing environment.
Reason for Policy	Access to computing and network resources owned and operated by TU imposes certain responsibilities and obligations and is granted subject to university policies, and local, state, and federal laws. Acceptable use is ethical, reflects academic honesty, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of data, system security mechanisms, and individuals' rights to privacy and to freedom from intimidation and harassment. The purpose of this policy is to outline the acceptable use of the TU ResNet.
Definitions	<p>Residential Network (ResNet) – includes all network systems and services used to provide data, voice or video over Internet Protocol (IP) service within the residence halls. These include hardware items such as wireless access points, routers, switches, hubs, and cabling inside and outside each residence hall room, but also includes many infrastructure systems required to deliver services.</p> <p>Clean Access – system used to validate a computer's security posture prior to network access.</p> <p>Networked Entertainment Systems – includes gaming systems (e.g. XBOX, Playstation, Wii) and Digital Video Recorders (e.g. TiVo, Slingbox).</p>
Responsible Executive and Office	<p>Responsible Executive Jeff Schmidt Associate Vice President and Chief Information Officer (CIO)</p> <p>Responsible Office Office of Technology Services</p>
Entities Affected by this Policy	All ResNet users
Procedures	<p>Access to the ResNet at TU is a privilege and must be treated as such by all users of these systems. Each user must accept the responsibility for their actions and agree to all parts of this policy.</p> <p>No personal network hardware additions</p> <ul style="list-style-type: none"> • Campus network equipment and wiring may not be modified, tampered with or extended for the purposes of redistributing ResNet access wirelessly or wired. • Personally-owned network devices (e.g. wireless access points,

switches, routers, etc.) are prohibited.

- Establishing a server of any kind is prohibited. Some examples are: FTP, Web Servers, e-mail servers, MP3, copyrighted media servers, and KaZaa or similar programs.
- Distribution of recorded, streamed or live TV or copyrighted video material is prohibited.
- Networked entertainment systems are permitted and are required to be registered with OTS. However, they may not act as a network routing device or network server for the purposes of hosting games, data or video to Internet based sources.
- The sole use of Webcams is for personal communications such as peer-to-peer chats. All other use is prohibited.

No malicious activity

- Scanning for insecure, vulnerable computers on any network, using port scanners or using network probing software, including packet-sniffing software, is strictly prohibited.
- The use of any hacking software and attempts to illegally connect to any other computer system or device is prohibited.
- Attempting to circumvent Clean Access or bypass system scanning for required patches and software is prohibited.
- Users of ResNet shall not intentionally disrupt network activity, attack machines on ResNet or the Internet, or capture private data of other users.

Adhere to laws and policies

- Users must comply with all federal, state, and local laws and ordinances including U.S. copyright laws. Illegal use and/or distribution of copyrighted materials such as computer software and music is prohibited.
- Users shall not use their connection to harass abuse or threaten other users with bodily harm, either on campus or across the Internet.
- Use of ResNet connections for commercial purposes, either for-profit or non-profit, is prohibited.
- Users are responsible for all activities traced to your user ID or that originate from your computer(s) or network devices. This includes guests.
- ResNet users must abide by the TU Acceptable Use and Information Technology Security policies.

Adhere to privacy and personal protection

- Users must keep their personal computers up-to-date with security

- patches and operating system updates.
- Protect your user ID and system from unauthorized use.
- Every computer connected to the ResNet must run anti-virus protection software with up-to-date virus definitions. TU provides McAfee anti-virus software free of charge for student use.
- All e-mail sent via the ResNet must accurately identify the sender. Sending anonymous e-mail or bulk, unsolicited e-mail (SPAM) is prohibited.
- Use of equipment to receive unauthorized video services is prohibited.
- The ResNet is a shared resource. Network use or applications that inhibit or interfere with the use of the network by others is prohibited. Users may be asked to cease any system activity that directly or indirectly causes a problem on the network.

Disclaimer

ResNet users connect to the network at their sole risk. TU will not be responsible for damage to or loss of hardware, software or data stored on computers located on the university property or connected to the network.

Reporting Violations

All suspected violations must be reported immediately to the proper authorities. For alleged violations, contact the Information Security Officer at incident@towson.edu.

Enforcement

Anyone found to be in violation of this policy may face disciplinary action as specified in the Student Handbook and applicable university policies, and procedures. Revocation or restriction of computer and network privileges is also possible. Offenders also may be prosecuted under applicable local, state and federal laws. The Information Security Officer reserves the right to audit computer and network systems on a periodic basis to ensure compliance with this policy.

<p>Related Policies</p>	<ul style="list-style-type: none"> • OTS IT Policies, Standards and Guidelines • IT Security Policy • Acceptable Use Policy
<p>Approval Date</p> <p>Effective Date</p>	

