Network and Personally Owned Devices Connection and Support Policy

Category: Operations; Students and Teaching

Approval: PVP

Responsibility: AVP-Information Technology

Approval Date: October 11, 2016; revised April 22, 2024

Definitions:
"User(s)" are defined as operators of computing devices. Every computing device connected to the network has an associated owner (e.g. a student who has a personal computer) or caretaker (e.g. a staff member who has a computer in their office). For the sake of this policy, owners and caretakers are both referred to as Users.

"Computing Devices" or simply "Devices" is a term inclusive of any technology that connects to our network (whether personally owned or owned by the university), including, but not limited to, desktop computers, laptops, servers, wireless computers, mobile devices, smartphones, specialized equipment, cameras, environmental control systems, wearable devices, and telephone system components.

"Appropriate Connectivity Points" is defined as the methods by which a user, through their device(s), can connect to the network. For the purposes of this policy, this includes Trent voice/data jacks, Trent's wireless network access points (Eduroam and ResNet), or via remote access technologies (e.g. VPN or SSH tunnel as approved by the IT department).

Personally owned devices – Devices that are owned or managed by individual members of the Trent community and are not IT managed as defined below.

Information Technology (IT) managed devices– Devices that are procured and managed by Trent IT as part of the University's fleet of computing devices. These devices are connected to IT-provided central management services for updates, security, and software distribution.

Servers – Devices that offer accessible services inside the Trent network or to the internet.

Internet only network – A portion of the Trent network where users can only access the internet as well as any Trent services available to the public.

Instrumentation Network – A portion of the Trent network dedicated to the connection of instrumentation devices for research purposes.

Internal limited network – A portion of the Trent network where some additional internal services may be accessible in addition to internet access. This network is designed to accommodate devices that are not IT managed but still require some access to network resources while balancing the need for security.

Full network access – Access to the internal Trent network and all services hosted by Trent IT as well as access to the internet.

Purpose/Reason for Policy:
This policy is designed to protect the campus network and the ability of members of the Trent community to use it. The purpose of this policy is to define the standards for connecting computing devices to the University's network and to determine the scope of support Trent IT will provide for equipment not provided by IT. The standards are designed to minimize the potential exposure to Trent University and our community from damages (including financial, loss of work, and loss of data) that could result from computing devices that are not configured or maintained properly and to ensure that neither computing devices nor users on the network are taking actions that could adversely affect network performance.

Trent University must provide a secure network for our educational, research, instructional and administrative needs, and services. An unsecured computing device on the network could allow denial of service attacks, viruses, Trojans, or other such risks to compromise the University's network, potentially affecting many computing devices. A violation of our network's integrity could result in the loss of sensitive and confidential data, interruption of network services and damage to critical internal systems.

Universities that have been severely compromised have also experienced reputational damage and a loss of confidence by users in the security of their privacy, data, and security. Therefore, individuals who connect computing devices to Trent's network's must follow the directions outlined in this policy.

Scope of this Policy:
This policy applies to all members of the Trent University community as well as to any visitors who have computing devices connected to the Trent University network. The policy also applies to users who have computing devices that access the campus network and resources remotely. The policy applies to University-owned computing devices (including those purchased with grant funds), and personally owned or leased computing devices that connect to the Trent network. The policy does not apply to devices which only connect solely to publicly available university resources through the World Wide Web.

Policy Statement:

Appropriate Connection Methods
Users may connect devices to the campus network at appropriate connectivity points. Modifications or extensions to the network can cause undesired effects, including loss of connectivity. These effects are not always immediate, nor are they always located at the site of modifications Therefore, extending or modifying the Trent network (e.g. through the addition of switching equipment or routers) must only be done by, or with the guidance of, the IT department.

Network Registration
Users of the University network may be required to register a device before connecting it. Users may also be required to install a software agent on their device before they are allowed on the network. The role of such an agent would be to ensure that the device complies with current standards.

Responsibility for Security
Users are responsible for ensuring that their computing devices meet all relevant security standards and for managing the security of the equipment, software and services that run on it. Some departments may assign the responsibility for computer security and maintenance to dedicated departmental staff. Therefore, it is possible that one user could manage multiple departmental devices plus their own computing devices. Every user should know who is responsible for maintaining their computing device(s).

Security Standards

Users must ensure that all computing devices are capable of meeting the appropriate safeguards for protection as determined by Trent IT.

Users must install the most recent security patches to the computing devices for which they are responsible as soon as practical or as directed by Information Technology. Where computing devices cannot be patched, other actions may need to be taken to secure the computing devices appropriately or else such devices may be moved to a network with more limited access.

Users must take care to ensure that devices connected to the Trent network and used to access sensitive information meet the requirements outlined in the Handling Sensitive Electronic Information Policy for the type of information they may be accessing, storing, or transmitting.

Central Network-Based Services

Information Technology is responsible for providing reliable network services for the entire university community. As such, users or departments may not run any service which disrupts or interferes with IT- provided services. These services include, but are not limited to, email, DNS, DHCP, and Domain Registration. Exceptions may be made by IT for approved personnel in departments who have demonstrated their competence in managing such services. Also, users or departments may not run any service or server which stores or processes Trent usernames and passwords.

Connections to the Trent network

Only devices that are supported and maintained by Trent IT can be connected to full network access including VPN and remote connection points.

Users who wish to connect personally owned devices to a limited access network, as defined above, must register the devices with Trent IT, install software agents and meet IT's minimal standards and requirements for such devices.

Protection of the Network

Information Technology uses multiple methods to protect the Trent network, including:

- monitoring for external intrusion
- scanning hosts on the network for suspicious activity and anomalies
- blocking harmful traffic, both inbound and outbound
- Using 24x7, AI based and machine learning anti-threat protection software
- Installing automated tools and firewall policies that restrict communication between network devices

Information Technology routinely scans the Trent network for vulnerabilities and signs of compromise, and computing devices connected to our network may be scanned for possible vulnerabilities.

Trent University reserves the right to take necessary steps to contain security exposures to its network. Information Technology or our contracted service providers may take immediate action to contain devices that compromise the operation or security of Trent's network including those listed below

- imposing an exceptional load on a campus service
- exhibiting a pattern of network traffic that disrupts centrally provided services.
- exhibiting a pattern of malicious network traffic associated with scanning or attacking others.
- exhibiting behaviour consistent with a host compromise

Normal traffic to devices that have been contained to safeguard the operation or security of Trent's

network will be restored after any underlying security vulnerabilities or issues have been remediated to the satisfaction of Trent IT.

Decryption of Traffic

The encryption of information to mask attacks is becoming increasingly common. For the purpose of monitoring the network for security vulnerabilities only, Trent IT may require users who have full access to the Trent network to install agents, keys, or certificates that may decrypt traffic so such traffic can be evaluated for security issues. The university will ensure that decrypted data is not retained longer than necessary for security purposes.

Hosting services and servers to the internet via the Trent network.

Devices connected to the Trent network that provide inbound or internet available services (servers) must be co-managed by Trent IT with a documented service level agreement that clearly delineates of responsibilities. Departments or users who wish to provide such services must install appropriate security measures, as required by Trent IT, and maintain minimum standards as defined by Trent IT and outlined in the service level agreement.

Instrumentation Network

An isolated and limited access portion of the Trent network is available to connect computers directly attached to instrumentation devices for the purposes of facilitating data exchange with said devices. Because devices connected to this network may be unable to obtain updates or patches, Trent IT may take reasonable steps to isolate a limited access network from other network services as defined above. Devices that operate as internet servers to the broader public may not be hosted on the instrumentation network.

Support and assistance from Trent IT.

The IT service desk will provide reasonable assistance to members of the Trent University community who wish to use personally owned devices for work and study purposes consistent with this policy and the Handling Sensitive Electronic Information policy. However, Trent IT cannot guarantee connectivity for nor provide extensive repair services or configure devices that are not university-owned and managed by Trent IT. Additionally, Trent IT cannot support internet services that are not provided by the University such as home internet providers or cellular networks.

Support and assistance from Trent IT for instrumentation devices.

IT will provide reasonable assistance to members of the Trent University community with the general repair, upkeep and maintenance of computers that are directly connected to instrumentation devices at the University. However, given the complexities of this equipment, the age of the devices and the availability of suitable replacement hardware and software, Trent IT cannot guarantee connectivity for nor provide extensive repair or configure devices connected to instrumentation.

Information Technology reserves the right to take the necessary steps to contain security exposures to the University network for any other reason.

Contact Officer:

Associate Vice-President-IT

Date for Next Review:

April 2026

Related Policies, Procedures and Guidelines

- Handling Sensitive Electronic Information Policy
- Computing Resources Acceptable Use Policy
- User Electronic Information Access Policy
- Computing Privileges Policy

Policies Superseded by this Policy:

- Guidelines for Use of Information Technology