

Appendix To Policy A21 – Acceptable Use – Telephone, Computing and Network Resources

APPENDIX A - UNACCEPTABLE USES

The following activities are prohibited unless they are part of legitimate job responsibilities:

No user is permitted to use the resources to engage in any activity that is illegal under local, provincial, federal or international law. No user is permitted to use the resources to engage in any activity that violates Olds College policies.

The list below is not exhaustive but serves as a framework for the types of activities which are unacceptable.

1. Violating the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations. This includes software products that are not appropriately licensed for use by Olds College.
2. Unauthorized copying of copyrighted material.
3. Exporting software, technical information, encryption software or technology in violation of international or regional export control laws.
4. Introducing of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
6. Using an Olds College computing asset to procure or transmit material that is in violation of the Olds College Harassment Policy or hostile workplace laws.
7. Making fraudulent offers of products, items, or services originating from any Olds College account.
8. Making statements about fraudulent association with Olds College including but not limited to unauthorized use of the Olds College logo.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access. Disruption includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
10. Port scanning or security scanning is expressly prohibited unless prior notification to Olds College is made.
11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

12. Circumventing user authentication or security of any host, network or account.
13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
15. Providing information about, or lists of, Olds College employees and students to parties outside Olds College without written consent.