

UWinId Request Form

Student Club, Association or a Society Affiliated with the University of Windsor

To be completed by requestor/person responsible for the account:

First Name:	Last Name:
Student Number:	UWin id:
Department:	
Club Name:	Requested Club UWin id: (length - between 3 – 8 characters, no special characters or spaces) Choice 1: Choice 2: Choice 3:
Length of Time Account will be required (max 1 year) - From: _____ To: _____	

I am requesting a Computer UWin ID to be used by our organization for the purpose of communication. I have read and understood the University of Windsor, Information Technology Services Acceptable Use Policy, documented on the back of this form. If a UWinID is issued, I will be solely responsible for the UWinID and will not give this id and password to any other person. I will use this UWinid for the activities of our organization only and will cease using it at the end of my term of office.

I understand that IT Services will de-activate this account during the change of officers at our organization but will keep the files for the use of any future officers of our organization for a maximum period of 12 months. After that time, the files may be deleted from the system.

When the term or position changes within the organization, the new person/officer will be responsible for coming to the IT Services HelpDesk to complete a new form.

Requestor Authorization

Signature: _____

Date: _____

Attestation

by the President, University of Windsor Students' Alliance or a Faculty Member

Signature: _____

Date: _____

University of Windsor

Computing and Networking: Acceptable Use Policy

General Principals:

1. The Computing and networking facilities of the University of Windsor support instructional, research, public service and other intellectual pursuits by students, faculty and staff that is consistent with the university's mission.
2. Since campus network services enable open scholarly communication on a world-wide basis, they are subject to the acceptable use guidelines established by regional and national networks (er Onet and the Internet). Individuals who make use of these external networks should familiarize themselves with the application guidelines, copies of which are available from Computing Services.
3. Anyone using an external network or an administrative system requires an unique ID and password.
4. The holder of a computer ID and password is responsible for protecting campus computing facilities from unauthorized access by keeping the password confidential and by changing it regularly.

Acceptable Use:

Generally, any computing or network communication activities which fall within these general principals are considered acceptable use of campus computing and networking facilities.

Unacceptable Use:

Confirmed incidents of unacceptable use will result in a sanctions ranging from verbal warnings to revocation of computing privileges, to expulsion and criminal prosecutions.

Unacceptable uses include:

1. Uses that violate federal or provincial laws, or university bylaws and policies such as those concerning information confidentiality.
2. Any uses that unduly interfere with the work of others or with the work of the host or password; seeking information about or attempt to modify the University's computer security system; and knowingly propagating computer viruses or electronic chain letters.
3. Unauthorized copying of proprietary software, publications or files.
4. Uses of commercial software that in any way violate the applicable licensing agreement.
5. Uses related to commercial activities including, but not limited to distribution of advertising material, offering network information or services for sale or personal gain and private enterprises.
6. Computer information that portrays either men or women or their body parts in a pornographic or derogatory manner.