U of G | Office of Registrarial Services

Access Request for "Class Lists"

Return the completed form by email to clistauth@registrar.uoguelph.ca
The intended user must read and sign the Acceptable Use Policy on the reverse side of this form.

To be completed by the 'End User' Department

Date of Request: _____

Last Name: _____ First Name: _____

Employee ID: _____ Central Login: _____

Position Title: _____

Date Access is Needed: _____
(Please allow up to 5 business days for processing once received.)

Explain your business need for accessing the information available through Class Lists:

☐ Final grade upload

☐ Other (specify below)

Are you replacing another user? ☒ Yes ☐ No

If yes, who? (Provide central login or full name) _____
(Please note that if you are replacing another user that individual's access will be disabled upon the activation of this new account.)

If yes, why? _____

Supervisor Name: _____ Supervisor Title: _____

Supervisor Signature: _____ Date: _____

To be completed by the Office of Registrarial Services

Director or Designate Approval: _____ Date: _____

Special Capabilities or Restrictions: _____

Date of User ID Assignment: _____ Date of User Notification: _____

Colleague ID: _____

University of Guelph
Acceptable Use Policy for Information Technology

The University of Guelph authorizes the University community to use its Information Technology Resources to fulfill and advance the University's teaching, learning, research, service, administrative, and community development missions.

In addition, the University permits limited personal use of these resources, provided this use does not violate any law, statute, or University policy. Users who require a private means of computing and sending electronic communications should utilize a personal device unconnected to the University's IT network**.**

The University respects the privacy of all users of its IT Resources, and uses reasonable efforts to maintain confidentiality of Personal Information. Circumstances may arise in which such privacy cannot be maintained. Such circumstances include, but are not limited to:

1. Access to Personal Information may be granted to an Authorized User, System Administrator, or agent to meet legitimate University business needs and operational requirements, or in the event that an Authorized User is unavailable, or has his or her access revoked.
2. The University may audit, access, or restore any IT resource within its environment when it has reasonable grounds to suspect a breach of acceptable use or a possible violation of any law or University policy.

Such access will be subject to the authorization of the appropriate Vice-President (or designate) in consultation with the Provost.

Authorized Users must exercise good judgment in determining what is acceptable use of IT Resources with due regard to this policy, other University policies and Community Standards. Some activities may be appropriate in a specific context (e.g. for authorized academic and research purposes), while some are not appropriate in any context.

Authorized Users have an obligation to take all reasonable steps (e.g. password protection and strengthening) to protect the confidentiality, integrity, and availability of IT Resources and report encountered vulnerabilities to the Information Technology Security Officer. Failure to do so may constitute a breach of this policy.

Examples of a Breach of Acceptable Use

Unless explicitly authorized, a breach of acceptable use includes, but is not limited to:

1. Allowing others to access your assigned personal Account
2. Failure to exercise reasonable care in safeguarding Accounts and information
3. Accessing someone else's personal Account
4. Seeking information on passwords or information belonging to others
5. Breaking or attempting to circumvent licensing or copyright provisions
6. Copying, deleting, intercepting, or examining someone else's files, programs, or information
7. Attempting to collect, use, or disclose, the Personal Information of others
8. Using IT resources to harass or bully others
9. Attempting to circumvent information security provisions or exploit vulnerabilities
10. Using IT Resources (e.g. University computing account or workstation) for unauthorized commercial purposes
11. Any interference with the ability of others to use IT Resources whether it is disruptive or not
12. Falsifying or misrepresenting your identity
13. Viewing or using pornographic or offensive material in a work, study, or public location
14. Distributing or disseminating pornographic or offensive material in any location

The above represents a segment of the Acceptable Use Policy for Information Technology.

I have read and understand and agree to abide to the Acceptable Use Policy for Information Technology.

Signature: _____ Date: _____

Name: (Please print) _____ Dept. Name: _____