Network User ID Policy

Affiliation Requirements

Community College of Allegheny County (CCAC) requires that people creating and using a Network User ID meet one of the following criteria:

- currently enrolled
- currently employed
- retired from the College

Employees who are retiring should send an email message to helpdesk@ccac.edu in order to continue the use of their Network User ID.

Single User ID Policy

CCAC Information Technology Services (ITS) grants one Network User ID per person for access to a variety of services including file and printer sharing and email. Services requiring a User ID can be accessed with the same User ID and the same password. This provides greater system security, better performance, and simplifies Network resource allocations.

Ethical Standards

Network Users are expected to follow conventional standards of ethics and polite conduct in their use of computing resources. It is expected that users will behave responsibly, ethically, and politely, even in the absence of reminders or enforcement.

Terms of Agreement for Network User IDs

Users are solely responsible for the use of their CCAC Network User ID, the resources to which your User ID provides access, activity on the network that can be traced back to your account or computer, and for the content of any information you make available through use of these resources. All such activity is subject to the laws of the State of

Pennsylvania and the United States, as well as the policies governing the Community College of Allegheny County.

By accepting computing and network privileges and continued access to these resources, you are also accepting the following terms of agreement:

- Access to computing and network resources granted through the issuing of a CCAC Network User ID may be used only by the specific individual to whom the User ID is issued and may not be shared with other individuals.
- An individual's personal data and use of the network are considered private, but personal data and network activity may be reviewed by ITS staff or administrative personnel under certain circumstances. Such circumstances include, but are not limited to, the specific request of the owner of data for staff to examine content; the administration of a system or the network requiring special intervention; and suspicion of ethical or legal violations that staff members with proper security authorization are compelled to investigate.
- Access to computing and network resources is intended to support the College's mission and must be used in an ethical and legal manner consistent with all CCAC policies.

Legal, Ethical, and College Policy Prohibitions

The following list of prohibitions is meant as a representative sampling and is by no means intended to provide a comprehensive collection of legal, ethical, and College policy violations.

Activities prohibited when using CCAC computing and network resources include, but are not limited to:

- Harassment (which is defined in the Campus Honor Code);
- Any commercial or for-profit ventures (such as running a business using your campus web space, email account, or network access);
- Disrupting a system or the network or preventing authorized access of such resources for use by others (including sending "chain letters" and consuming excessive system or network resources);
- Access, attempted or successful, to resources for which you do not have proper authorization;
- Distribution of pornography;
- Possession, accessing, or distribution of obscene material;
- Copyright violation (including possession or distribution of written, graphic, video, music or other media, such as MP3 files, which you are not legally authorized to possess or distribute).

Consequences of Misuse

Violations of the above terms of agreement may result in suspension of computing privileges, disciplinary review, termination of employment, and/or legal action. ITS will refer serious violations to the appropriate department for disciplinary action.

Forgotten Passwords

Forgotten passwords for Network User IDs are reset at their respective Campus. User ID security precautions require a personal visit and a picture ID.

User ID and Data Expiration

User IDs will be terminated once a person is no longer affiliated with the College. However our practice is to allow continued access for three months to ameliorate the potential impact on faculty and staff who may temporarily lose their official affiliation for short periods of time. Unless affiliation is officially reestablished, data will be deleted after three months.