
communications. Such laws and policies prohibit, among other things, lewd or indecent conduct, threat of physical harm, stalking, forgery, disruption of College services, damaging or destroying of property, discrimination and sexual harassment. All users are expected to respect the integrity of all security controls and abide by all security measures that have been implemented, as well as adhere to all end-user license and contractual agreements associated with Century College IT resources.

Cooperation with Investigations

Depending on the nature and severity of an alleged violation, Century College may notify the appropriate campus or external authorities for further investigation and possible disciplinary action or prosecution. Users violating Century College policies or state and federal laws may be subject to prosecution. While Century College technical staff members strive to provide reliable and secure IT resources, users should not consider the data storage or transmission systems to be secure and/or private.

Any data stored or transmitted using Century Colleg

Principles of Responsible IT Use

The following principles and examples are intended to illustrate some examples of unacceptable actions rather than to exhaustively list every specific behavior that may violate the Acceptable Use Policy. These principles are derived directly from the same standards of common sense and decency that apply to the use of any public resource.

-
-
- host a commercial web page;
 - allow anyone who does not have authorized use to access any IT resource or service;
 - conduct political campaigns;
 - operate unauthorized information services.