3358:11-4-10 Responsible computing policy.

(A) Purpose. Owens Community College provides access to distributed and local networked resources as a service to the campus community. It is the intent of the college that all technology resources will be used in accordance with any and all local, state and federal laws, and/or guidelines governing the use of information and technology with this and other policies and procedures of the college and with standards of professional and personal courtesy and conduct.

(B) Guidelines.

(1) It is expected that all students, faculty, and staff will utilize the information and technology resources of the college so as not to waste them, abuse them or interfere with or cause harm to other individuals, institutions or companies.

(2) Access to the college's information and technology resources is a privilege that may be wholly or partially restricted by the college without prior notice and without student/faculty/staff consent when required by and consistent with law, when there is substantiated reason to believe that violations of policy are taking place or when required to meet time-dependent critical operational needs.

(3) The college's information and technology resources, including all electronic mail addresses and user accounts, are the property of the college. The college does not uniformly or systematically monitor use of email or the internet. It does, however, maintain the right to do so if in receipt of a court order, public records request, freedom of information request, allegations of harassment or other similar type of situation.

(4) Account holders are responsible for maintaining the confidentiality of their password(s). Account holders must only use their account(s) and not use any other account. The information and technology resources of the college are intended for the use of students, faculty, and staff of the college. Account holders may only use accounts, files, software, and computer resources that are assigned to them under their user account(s). Account holders are expected to take all reasonable precautions to prevent unauthorized access to files and data and any other unauthorized usage within and outside the college.

(5) Both law and college policy prohibit, in general, the theft or other abuse of information and technology resources. Such prohibitions include, but are not limited to, unauthorized entry, use, transferring, tampering with accounts and files of others; interference with the work of others and with other computing facilities. Mischievous abuse of electronic mail and electronic campus information services that interferes with productivity or computer operations may result in suspension of computing privileges. Substantiated complaints regarding use of profanity, obscenity or offensive material may be cause for suspension of computing privileges.

(6) Attempting to circumvent security or administrative controls and/or assisting someone else or requesting someone else to circumvent security or administrative controls is prohibited.

(7) The college's information and technology resources are provided to support the teaching, research, and public service mission of the college and the administrative functions that support this mission. The college's information and technology resources must be used appropriately and only after receiving appropriate training. By completing the required training, the security and privacy requirements of the application are acknowledged.

(8) Upon termination of employment or job responsibilities and/or as requirements change, access to information resources will be changed or terminated.

(9) A person who files a complaint or participates in investigations shall be protected from any form of retaliation arising out of the filing of the complaint or participation in the investigation. A person who impedes an investigation, covers up the truth or retaliates against a complainant shall be subject to disciplinary action.

(10) The college may, from time to time, develop and publish procedures and practices that implement this policy.

(11) Penalties for actions which violate this rule will be assessed through existing disciplinary channels, up to and including termination.

Effective date: March 5, 2002

Daniel R. Hauenstein
Certification

February 19, 2002
Date

Promulgated under:	RC Sec. 111.15
Statutory authority:	RC Sec. 3358.08
Rule amplifies:	RC Sec. 3358.08
Prior effective dates:	N/A