CP – 8.1.1
ACCEPTABLE USE

Related Board of Trustees Policy: BP 8.1
OPR: Vice President for Administration
Approved: September 28, 2021
Previous Editions: February 21, 2006; April 18, 2006; December 9, 2013; August 5, 2015; December 1, 2015; December 5, 2017; November 27, 2018

ACCEPTABLE USE

College owned or operated Information Technology resources ("IT Resources") are reserved for the educational, instructional, research, and administrative computing needs of employees, students, contractors, third-party vendors, and other individuals authorized by the College. The IT Resources include, but are not limited to, all College computers and related hardware, access to Internet or intranet provided through College owned or operated computing and networking resources, online and offline storage, and all other communications media. Access to IT Resources is privileged. Users must exercise responsible and ethical behavior. Users must read, understand, acknowledge their understanding of this Procedure, using Form 8.1.1a, *Acknowledgement of Acceptable Use Policy and Procedure*.

The College monitors user access and reserves the right, without prior notice, to acquire and maintain all user logs and documentation retrieved from IT Resources. Users do not have an expectation of privacy regarding their use of IT Resources. Users give express consent to the College for monitoring, access, and evaluation. Information contained on the College's IT systems and in all College accounts, including but not limited to email, may also be subject to inspection as required by Public Records Laws of the State of North Carolina.

The College does not attempt to articulate all required or unacceptable behavior by its users. The College reserves the right to evaluate users' judgment and actions while accessing IT Resources.

The College is not liable for actions of anyone connected to the Internet through the College's IT Resources. All users assume full liability; legal, financial, or otherwise, for their actions.

IT Resources are strategic assets of the College and must be treated and managed accordingly. This Procedure:

- Establishes minimum appropriate and acceptable requirements regarding the use of IT Resources connected to the College network;
- Requires user compliance with applicable state laws and other rules and regulations regarding the management of IT Resources;
- Establishes training requirements for personnel who use IT Resources; and,
- Requires users acknowledge and agree to adhere to rules of behavior before gaining access to IT Resources connected to the College network.

This procedure incorporates the policies required by the North Carolina Department of Information Technology Acceptable Use Policy (AUP). It applies to all departments, employees, and students of Craven Community College not specifically excluded by NCGS 143B, Article 15. This Procedure will be reviewed by the Vice President for Administration and the Dean of Technology Services at least annually.

Acceptable Uses of Information Technology Resources

Acceptable uses of IT Resources include, but are not limited to:

- Official work of the College, instruction, academic research, independent study and professional development; and,
- Occasional non-commercial personal use, provided it does not otherwise violate a provision of this or any other policy of the College. Personal use is authorized when there is no cost to the College, does not interfere with official duties, and is infrequent.

Unacceptable Uses of Information Technology Requirements

IT Resources shall only be used for lawful purposes, and not be used for any purpose which is or could be reasonably perceived as deemed illegal, immoral, unethical, dishonest, or damaging to the reputation to the College. Actions inconsistent with the mission of the College, or any purpose that may subject the College to liability are unauthorized.

Unacceptable uses of IT resources include, but are not limited to:

- Political purposes or the sharing of personal beliefs/agendas;
- Personal or private gain, or for other activities in violation of the College's student or employee policies, unless such gain is incidental to the performance of official duties;
- Unauthorized access to other user accounts, access codes, passwords, network identities, email addresses, or any other credentials;
- Sharing of access credentials outside the College network or with any third parties. The sharing of account information, including passwords or any other access control credentials is strictly prohibited;
- Creation, access, or transmission of inappropriate material, including, but is not limited to, material that is obscene, illegal, offensive, libel, slanderous, cyberbullies, defames, or harasses;
- Creation, access, or transmission of inappropriate material, including, but is not limited to, material showing aversion, denigration, or hostility towards any protected class, including but not limited to, race, color, sex, pregnancy, national origin, disability, genetic information, age, religion, marital status, sexual orientation, gender identity, political beliefs, veteran status, or any other characteristic or classification protected by any applicable laws or policies;
- Misrepresentation of the College;
- Infringement of copyrights or trademarks;

- Providing, or attempting to provide, unauthorized access to IT resources, restricted portions of the network, an operating system, security software, or other administrative applications without authorization by the Dean of Technology Services via submission of a Help Desk ticket;

- Student access (excluding student employees) of employee computing devices, regardless of whether or not they contain sensitive data or are connected to the College's secure network;

- Activity that might be reasonably expected to degrade the performance of IT resources, deprive an authorized user access to IT resources, obtain extra resources beyond those allocated, or circumvent College information security Policies, Procedures, and Processes;

- Utilization of any unauthorized file sharing software, programs, applications, or services that incorporate file sharing to store Personally Identifiable Information (PII) or information classified as Sensitive by the data owner. Examples include, but are not limited to, Dropbox, Box, Google Drive, or Amazon S3 Storage. Requests for authorization are submitted to the Dean of Technology Services via a Help Desk ticket;

- Wasting, monopolizing, interfering with, or misusing IT Resources. Examples include, but are not limited to, requesting an excessive number of copies from a printer, playing computer games, and participating in chain letters;

- Destruction or damage to any portion of IT Resources, including paper and digital IT Resource records;

- Connection of unauthorized personal devices or non-College software or applications to the College network. Requests for authorization are submitted to the Dean of Technology Services via a Help Desk ticket. This requirement does not apply to users who connect to the College network through the College's "guest" (PantherNet) Wi-Fi network; and,

- Downloading, installing, or running security programs or utilities such as password cracking programs, packet sniffers, or port scanners that reveal or exploit weaknesses in the security of IT Resources.

Associated Handbooks and Forms

- 8.1.1a. *Acknowledgement of Acceptable Use Policy and Procedure*