9.2 ACCEPTABLE USE POLICY

Original Date of Issue: 5/15/96
Revised: 12/2014, 2008, 2000, 5/20/2026

1. Purpose

This Acceptable Use Policy ("Policy") defines the governance requirements for behavior while using the Delaware County Community College ("DCCC") Information Technology ("IT") systems and environments. Maintaining a secure information environment is a DCCC strategic objective. DCCC Administration demonstrates its commitment to information and cyber security through the maintenance of this Policy and associated policies and procedures.

2. Scope

This Policy applies to all authorized users of DCCC information systems and environments, including DCCC-owned infrastructure and third-party platforms contracted by DCCC. It defines acceptable use requirements for DCCC information systems, accounts, assets, and data. The DCCC environment is comprised of DCCC-controlled domains and platforms used to facilitate DCCC processes under DCCC control.

3. Definitions

See Glossary (https://catalog.dccc.edu/policies-procedures/administrative-computing/) for additional definitions

DCCC Mission is the academic and business mission of DCCC that drives its activities and policy structure.

4. Roles and Responsibilities

Accountable

Vice President ("VP") of Finance and Administration: The VP of Finance and Administration is ultimately accountable for the maintenance of this Policy and the establishment of implementing procedures but may delegate implementation of this policy to the VP of IT (defined below).

Responsible

Vice President of Information Technology ("VP of IT"): The VP of IT is responsible for the day-to-day operation of this policy and implementing procedures.

Supportive

Human Resources ("HR"): HR ensures that this Policy is acknowledged by all employees and contractors within 30 days of beginning employment.

IT Team: The IT Team is responsible for ensuring acknowledgement is required within 5 business days of student access.

Department Heads: Department Heads ensure all personnel are appropriately trained on the information within this Policy.

Consulted

Department Heads: Department Heads are consulted in the establishment of this Policy and its implementing procedures.

Informed

All Authorized Users: All Authorized Users shall be informed of and acknowledge this Policy.

5. Policy

The purpose of computing systems at Delaware County Community College is to support the educational mission of the College in accordance with college policies and in a manner conducive to the overall academic climate. Unless otherwise specified, all provisions of this Policy apply to all Authorized Users. Additional requirements for specific user groups are identified where applicable.

Access Conditions

Access to DCCC computing systems is a privilege and only authorized users may access DCCC information assets and systems. All Authorized Users must acknowledge this Policy and adhere to all DCCC policies and procedures concerning use of the information system. Access may be revoked at any time in DCCC's discretion pursuant to all relevant policies and procedures. Authorized Users must ensure they uphold the confidentiality of DCCC data.

Google Workspace is offered by Google in conjunction with Delaware County Community College ("DCCC") primarily for use by students. Staff are encouraged to use Microsoft 365 for productivity and communication needs; staff who access Google Workspace do so with the understanding that the same administrative rights described below apply to their accounts. As administrator of this service, DCCC may:

- View statistics regarding your account, such as information concerning your last login or data storage usage.
- Change your account password, suspend, or terminate your account access and your ability to modify your account.
- Access or retain information stored as part of your account, including your email, contacts, and other information.
- Receive account information in order to satisfy applicable law, regulation, legal process, or enforceable governmental request.

DCCC also reserves the right to alter configurations and access to meet security and legal requirements.

Acceptable Uses

Access to DCCC resources is intended to be for express business or educational purposes; use for other purposes is prohibited unless explicitly allowed under this Policy or expressly permitted by the VP of IT.

Limited incidental personal use of DCCC systems is permitted as a narrow exception, provided such use is lawful, minimal, does not interfere with job or academic responsibilities, DCCC's mission, operations, or compliance obligations, does not consume unreasonable resources, and does not involve Sensitive or Confidential data. DCCC reserves the right to restrict or revoke incidental personal use as necessary to protect its systems, operations, or compliance obligations.

The following is an enumeration of acceptable uses of DCCC information assets:

- Network Uses
  - Accessing College systems via the Authorized User's assigned identification and authentication credentials.
  - Remote access to fulfill a job or academic function using DCCC approved remote access tools.
- Email Services
  - Use for a business or academic purpose.
- Data Access and Sharing

- Sharing data within or outside DCCC systems only when authorized, in accordance with the data classification and handling requirements defined in the Asset and Data Management Policy (9.9), and for a legitimate business or academic purpose.
- Only using college-provided instant messaging ("IM").
- Only using file sharing or cloud storage solution approved and provided by DCCC.
- Only using devices such as memory sticks, CDs, DVDs, and removable media after approval by the Information Security team.
- Only viewing student or personnel records (i.e., records protected by Family Education Rights and Privacy Act ("FERPA")) if authorized and ensuring those records stay in the appropriate, designated storage locations.
- Printing, copying, or physically removing Sensitive or Confidential data from DCCC premises only when necessary, and ensuring such data is handled securely, kept to the minimum necessary, not left unattended, and disposed of appropriately when no longer needed.
- Accessing and using only the information and systems necessary to perform authorized job or academic responsibilities, in accordance with the Principle of Least Privilege.
- Internet and Web Access
  - Accessing websites and web-based applications in a manner consistent with DCCC policies, applicable laws, and the acceptable and unacceptable uses defined in this Policy.
  - Streaming media in a manner that does not interfere with network performance or violate other provisions of this Policy.
- Legal and Productive Use
  - Using the system in accordance with all applicable laws, regulations, compliance obligations, policies, and procedures.
  - Promoting a safe, healthy, and positive academic and working environment.

Unacceptable Uses

Uses of information assets that pose a risk to DCCC's business operations, reputation, and compliance obligations are explicitly prohibited. Specifically prohibited activities include, but are not limited to:

- Network Use
  - Accessing the system with another User's identifiers and authentication credentials or providing the same to another User or a non-authorized user.
  - Leaving user accounts logged in at an unattended and unlocked computer.
  - Leaving passwords unprotected (i.e., writing it down).
  - Performing any unauthorized changes to DCCC IT systems or information.
  - Attempting to access data that they are not authorized to use or access.
  - Exceeding the limits of their authorization or specific business need to interrogate the system or data.
  - Connecting any non-authorized device to the DCCC network or IT systems.
  - Storing DCCC data on any non-authorized equipment.
  - Giving or transferring DCCC data or software to any person or organization outside the college without express permission or authority.
  - Remote access for reasons other than to fulfill a job function or using non-DCCC-approved methods to access DCCC systems remotely.
  - Obfuscating your geo-location to subvert security controls or access restrictions.
  - Using DCCC network resources to initiate outbound remote desktop, SSH, or direct connections to third-party systems, unless the connection is part of an authorized educational program or uses software explicitly approved by the Office of Information Technology.
  - Using DCCC systems or credentials to access systems, networks, or data belonging to other institutions or organizations without explicit authorization from both DCCC and the external organization.
  - Impersonating another DCCC user, department, or college official through email, messaging, or any other communication channel, including through the use of AI-generated content.
  - Using a personal hotspot, cellular tethering, or other personal network connection on a College device to bypass DCCC network controls or security monitoring while on DCCC premises.
- Email Use
  - No Sensitive or Confidential data may be shared in unencrypted emails.
  - Using the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
  - Forwarding emails from a "@dccc.edu" email account to personal email accounts, unless otherwise expressly approved (outside of personal HR emails).
  - Using the email system for solicitation, personal profit, political purposes, harassment, or sending anonymous messages is prohibited.
  - Sending bulk or mass emails outside of College-authorized communication systems without prior approval from the Office of Information Technology or authorized College Communications staff.
  - Data Access and Sharing
    - Downloading, installing, or distributing any software from the internet without prior approval of the Office of Information Technology.
    - Blogging and social media postings on behalf of DCCC are prohibited without permission.
    - Sharing DCCC data without permission and outside of the Asset and Data Management requirements (see 9.9).
    - Instant messaging ("IM") outside of DCCC-provided IM tools.
    - Using peer-to-peer file sharing protocols or applications (i.e., BitTorrent) to download, upload, or distribute content without authorization.
    - Use of file sharing or cloud storage solutions not approved by DCCC or not approved to store data of that classification.
    - Use of personally owned or free versions of products and services (i.e., SaaS platforms, personal AI subscriptions) with Sensitive or Confidential information.
    - Accessing, copying, modifying, or distributing another user's files or data without their consent or without authorization under this Policy.
    - Using unapproved devices such as memory sticks, CDs, DVDs, and other removable media.

    - Storing Sensitive or Confidential College data in personal instances of cloud storage platforms, including personal accounts on platforms otherwise approved for institutional use (i.e., personal OneDrive or personal Google Drive accounts).
- Internet and Web Access
    - Use of malicious websites, unauthorized web systems, or illegal online services that pose a security risk.
    - Circumventing DCCC controls access to blocked websites or web applications.
- Illegal and Harmful Uses
    - Engaging in activity that is illegal under local, state, federal, or international law.
    - Engaging in unlawful, fraudulent, harassing, discriminatory, deceptive, or otherwise unauthorized activity that harms or is reasonably likely to harm DCCC's operations, security, legal compliance, or reputation.
    - Introducing, downloading, installing, or knowingly executing malicious software, including viruses, ransomware, spyware, adware, keyloggers, trojans, or any other software designed to damage, disrupt, or gain unauthorized access to DCCC systems or data.
    - Sending or storing payment card data or other sensitive or regulated data on the DCCC network without authorization.
    - Using the internet or email for the purposes of harassment or abuse.
    - Disseminating vilifying, illegal, sexist, racist, abusive, harassing, discriminatory, threatening, obscene, or otherwise inappropriate messages or media.
    - Accessing, creating, downloading, sending, or receiving any data (including images) that include sexually explicit, discriminatory, defamatory, or libelous material.
    - Using college computing systems, licensed platforms, or internet access to make personal gains or conduct a personal business (i.e., crypto mining), including making fraudulent offers for products or services.
    - Making official commitments or representations through the internet or email on behalf of DCCC unless authorized to do so.
    - Downloading or making duplicates of any copyrighted material such as music media (MP3) files, film, and video files without express approval.
    - In any way infringing any copyright, database rights, trademarks, or other intellectual property.
    - Connecting DCCC devices to the internet using non-standard connections, such as personal Wi-Fi devices when DCCC connections are available.
    - Performing any of the following without authorization: port scanning, security scanning, network sniffing, penetration testing, or other IT information gathering techniques, unless authorized by the AVP of IT.
    - Conducting an activity that is intended to consume large amounts of college network bandwidth.
    - Attempting to circumvent or bypass security controls, authentication mechanisms, or user-based access restrictions, including unauthorized privilege escalation.

Awareness and Training

All Authorized Users must complete required training within the timeframe designated for their role, as established by the AVP of IT in implementing procedures. Failure to complete required training within the designated timeframe will result in account disablement at the discretion of the AVP of IT. Where applicable, DCCC retains records of training completion in accordance with the record retention schedule. Each Authorized User shall be trained annually based on their role. Training shall be customized to each user's role and contain the minimum attributes:

- Students must review and acknowledge the information security policies. Students may also from time to time receive awareness advisories based on observed risky behavior and other pertinent threats of which they should be aware.
- Faculty and Staff must complete periodic basic security awareness training modules, including phishing, clean desk/screen, and insider threat, and review and acknowledge security policies.
- Administrators must complete periodic basic security awareness training modules, including phishing, clean desk/screen, and insider threat; review and acknowledge security policies; and ensure all Authorized Users have completed training requirements.
- IT administrators and privileged users must complete periodic basic security awareness training modules, including phishing, clean desk/screen, and insider threat; review and acknowledge security policies; receive periodic training and updates on security basics related to their role and to address relevant security risks (unless they have received certifications on the same); and verify technical competency to fulfill their roles and responsibilities (i.e., firewall administration, secure architecture basics, etc.) and that IT administrators and privileged users have taken steps to maintain such competency. Competency can also be demonstrated by industry-recognized certification or other credentials earned prior to or during their tenure at DCCC.
- All users with legal, regulatory, or contractual compliance roles shall, in addition to the basic security awareness training, receive training on their responsibilities related to that role.

Monitoring and Incident Reporting

All activities conducted on college-owned devices, networks, and systems or applications licensed or provided by the College (e.g., cloud-based services) have the express expectation of monitoring for security and compliance purposes. Users have no expectation of privacy.

While the College does not routinely inspect or monitor electronic mail, messages on DCCC-provided email servers are subject to institutional scrutiny when authorized by DCCC officials as follows:

- To meet system administration/troubleshooting needs.
- To meet institutional needs.
- To meet external legal requirements.

Examination of messages to meet institutional needs or legal requirements will be performed by an authorized system administrator in conjunction with the AVP of IT, the Director of Safety & Security, and/or DCCC Legal Counsel.

Users who know or reasonably suspect a security policy violation, data breach, or unauthorized disclosure of Sensitive or Confidential information has occurred must immediately report it to infosec@dccc.edu. This includes but is not limited to attempted phishing attacks, potential insider threats, suspected exposure of FERPA-protected

records, PII, financial data, or authentication credentials, regardless of whether the exposure was accidental or intentional.

Users must immediately report lost or stolen devices that contain or may provide access to DCCC systems or data to infosec@dccc.edu.

Technology Acquisitions

All acquisitions of technology-related products, including but not limited to, computer-related hardware, software, technology services, telecommunication services, and audio-visual systems, regardless of cost, must be reviewed by the Office of Information Technology before entering into a new contract, a contract renewal, or direct ordering. This includes subscriptions to web-based or cloud-based services, telecommunication systems and services, and any service that includes or relies on a mobile application.

Departments should engage OIT as early in the process as possible to allow for review of the system or service, assessment of security and privacy requirements, and evaluation of compatibility with existing supported systems. OIT can also provide technical assistance in the review of proposed contracts, work plans, implementation services, and privacy policies.

No technology service or product may be procured or renewed without OIT review, regardless of funding source.

Artificial Intelligence

The use of artificial intelligence tools for college purposes must be reviewed and approved through the Office of Information Technology prior to use. Users may not use unapproved or personal AI tools with Sensitive or Confidential College data. Questions regarding approved AI tools should be directed to the Office of Information Technology.

6. Compliance

Failure to comply with this policy may result in sanctions in accordance with the Employee and/or Student Handbook and applicable laws and regulations, which may include termination of employment or enrollment. It is the responsibility of every individual user to report any known violations to the AVP of IT or the VP of Finance and Administration. Authorized Users who wish to report suspected violations confidentially, or who are concerned about potential retaliation, may do so through the College's Whistleblower Policy, which includes an anonymous reporting hotline at 855-832-5551 or www.dccchotline.ethicspoint.com.

- Inadvertent misuse of the College's computing systems, for example unintentional overload of systems or excessive disk consumption, will be handled by procedures of the College's Office of Information Technology.
- Violations by students will be reported to the Vice President of Student Affairs for review and resolution according to the procedures of the Student Code of Conduct as stated in the DCCC student handbook.
- Violations by staff will be reported to the Vice President of Finance and Administration, the staff member's supervisor, and to the Vice President of Human Resources for review and resolution in accordance with the College's personnel policies.
- Violations by the public will be reported to the Vice President of Finance and Administration for review and resolution. Penalty for violation may range from prohibition of access to DCCC's systems and facilities to the notification of law enforcement authorities.
- Account privileges and access to specific systems, services, or devices may be suspended, disabled, restricted, or terminated while a reported violation is under review or where a violation has occurred or is suspected, pending investigation and resolution.

Organizational compliance and efficacy of this Policy shall be reviewed periodically, as deemed necessary by the AVP of IT. The review, per the Information Security Policy (9.1), will include the following minimum attributes:

- Updates upon significant changes to the system or organizational requirements or in response to the results of a risk assessment;
- Consistency in implementation;
- Maintenance of implementing procedures; and
- Compliance with applicable laws and regulations.

Exceptions

Exceptions must be approved and documented by the DCCC Office of Information Technology. All exceptions shall be documented and reviewed during the next upcoming Risk Assessment. Please see the Information Security Policy (9.1) for additional information.

7. References

- 9.1 Information Security Policy
- 9.9 Asset and Data Management Policy
- ISO 27001:2022 Information security management systems — Requirements
- NIST SP 800-53 r. 5 Security and Privacy Controls for Information Systems and Organizations
- 16 C.F.R. Sections 314.3-314.4 (FTC Safeguards Rule)