Sussex County Community College
Policy No.: 102.3
Area: Information Technology
Adopted: 7/25/17

102.3 Technology Access, Use, and Data Security

PURPOSE OF THE POLICY

Technology being an essential, daily use component for staff, faculty, and students, the potential for abuse could have a dramatic impact on daily operations at the College. This being understood, the same ethical standards that apply to our non-technical, on campus environment apply within the electronic environment as well. In providing computing and data resources, SCCC has the responsibility of informing all technology users (staff, faculty, students, and visitors) of the policies and procedures regarding their usage. All users of technology are responsible for thoroughly understanding these policies and procedures and will be held accountable to them.

GENERAL STATEMENT OF THE POLICY ABOUT TECHNOLOGY ACCESS

Policies, pertaining to technology use conduct, generally address issues such as; appropriate versus inappropriate usage, theft, destruction of property or vandalism, data security, and level of access granted (i.e. what technology is available for use by an individual and when). The Technology Access, Use, and Data Security Policy is intended to address these elements as they apply to rapidly evolving technology of computing, networking, information resources, and social media. Because technology use and reliance is constantly expanding and changing, no electronic and/or data use policy can hope to remain current in all its minutiae. The policy outlined herein should be considered to contain examples for and not an exhaustive list of acceptable and prohibited behavior. Unauthorized or inappropriate technology usage carries with it multiple implications. It may mean that an individual is no longer authorized to utilize specific machines, networks and/ or other related resources, for any purpose. Alternately, it may mean that, although an individual is authorized to use a particular technology resource, certain activities or access, regarding its usage, will be prohibited.

ACCESS AND ACCEPTABLE USE OF ELECTRONIC RESOURCES

The responsible and ethical use of technology is essential on campus, as staff, faculty, and/or students may have access to several valuable resources. Inappropriate use practices can inadvertently affect not only the internal network, but may additionally have an expansive, negative impact on the workflow of other network users. While most users employ technology responsibly, the few who do not, either through ignorance or by intent, offer the potential of disrupting either individual or groups of other network users. Sussex County Community College has the responsibility of securing its networks, servers, and workstations to an economically feasible degree against unauthorized access, while maintaining accessibility for legitimate use requirements. Part of this accountability includes informing users of an expected standard of conduct and the punitive measures for not adhering to them.

As an academic community, the students, faculty, staff, administration, and guests of the College honor intellectual property, respect the privacy of data, and recognize the rights of others. Each individual has a right of access to a fair share of available computing resources and to the privacy of files, and each has the responsibility, in turn, to use resources in an ethical manner.

It is the intent of the College to provide high quality computing facilities to its users both to allow the College community to maintain its access to available local, national, and international information and to provide an environment which encourages both the acquisition of knowledge and the sharing of information.

All technology owned by the College shall be used in a manner consistent with the College's mission to support lifelong learning opportunities for student success. Each computer and all supporting technology infrastructure such as servers and networks within the campus community are tools belonging to the College. It is each technology user's responsibility to be familiar with the particular conditions of the use of, and to abide by, the computing provisions set forth within College policy, rules, and regulations.

The health and well-being of this resource requires constant vigilance by its users, who must all guard against any usage which disrupts and/or threatens the long-term viability of the systems at SCCC as well as those beyond the College. Sussex County Community College requires that members of its community act in accordance with these responsibilities, this policy, relevant laws, contractual obligations, and the highest standard of ethics

ELECTRONIC PRIVACY LIMITATIONS AND UNACCEPTABLE USE

As with all technology-reliant organizations, comprehensive network, systems administration, software and hardware support are essential components of the technical support directive. In coordination with best practices, constant monitoring and evaluation at all levels of the technical environment are carried out continually. Additionally, as a result of this essential process, and in coordination with security protocols, College computer systems, data, documents, email, and electronic communications are not private or confidential to the individual user. All equipment, documentation, and electronic communications are considered the property of Sussex County Community College.

SECURE DATA AND VIRTUAL PRIVATE NETWORK ACCESS

The privacy of student information contained in the Gramm-Leach-Bliley (G-L-B) Act is consistent with the privacy responsibilities that colleges and universities must follow under the Family Educational Rights and Privacy Act (FERPA). As such, Sussex Community College will protect the privacy of student records, including all financial records, to satisfy the Privacy Requirements of the G-L-B and FERPA, respectively. Sussex County Community College is committed to safeguarding student financial information, along with members of the campus community.

Sussex County Community College offers Virtual Private Network access (hereafter known as "VPN") accessible from the College website, secured through unique usernames, coupled with complex password requirements, and delivered through an encrypted interface. Access is limited by group policy management controls, setup and protected in compliance with network security protocols.

NETWORK USER ACCOUNT SAFEGUARDS AND ACCOUNTABILITY

To protect network security, accountability, and to enable secure group associations for access level controls, the College employs the use of individualized Network user access accounts to track and delineate data stored locally, on network shares, and through electronic mail.

SEPARATION OF EMPLOYMENT OR ENROLLMENT

Separation of employment or enrollment occurs when the contract with or enrollment of the individual is discontinued due to graduation, student enrollment discontinuance, or due to an employee's actions or the College's actions. The dismissal of a College employee from their job duties may be categorized as voluntary or involuntary. As part of this separation of employment or enrollment, the College realizes that an individual may have accrued personal intellectual property on College-owned devices, which they would like to retrieve during the separation process. The College will make reasonable attempts to retrieve personal intellectual property of a separated employee or student and will then make that personal intellectual property available to the separating individual.

COPYRIGHT MATERIAL COMPLIANCE

Sussex County Community College complies with the 1976 Copyright Act through the adherence of established guidelines and standards of educational fair use, as specified under Section 107 of H.R. 2223. The College strictly enforces all laws governing these guidelines and standards. All infractions will be directed to the Vice President of Administrative Services for review and disposition, forwarded through appropriate departmental management.

All copyrighted materials, obtained through College network resources, whether they be directly on College- owned devices or through the use of College network access, will be subject to all laws and guidelines set forth through state and federal statutes. Any individuals found to be obtaining copyrighted materials that such individual does not have a legal right to possess, such as but not limited to the use of peer-to-peer file sharing, Bit Torrent software or other similar software will be subject to review by the Vice President of Administrative Services, Human Resources, and in conjunction with appropriate departmental management. Appropriate action, as determined by the College in its sole discretion, shall be taken against all offending individuals, up to and including loss of network access privileges, termination of employment or expulsion, and criminal prosecution where applicable.