SUMMARY Electronic Mail and Electronic Communications Guidelines

October 2019

A guide for users of the College Electronic Communications Infrastructure

What is the Purpose of These Guidelines?
The College has made a significant investment in electronic communications technologies to increase capacity to accommodate more users and more applications and to provide higher quality service. These investments are intended to improve College instruction and instructional support for its students through use of electronic communications. Nonetheless, like books in a library or classroom space, there are restrictions that insure sensible use of the facilities to enable them to be used effectively and efficiently. Reliable operation, privacy, security and fair access are the goals. Should the College deem it necessary, it reserves the right to control usage through denying or restricting access to these facilities. These guidelines were put into effect to insure the reliable operation, privacy, security, and fair access of the college's electronic communications infrastructure.

What is Electronic Communication?
The college defines electronic communication as interactive and one-way electronics services that include, but are not limited too, voice telephony, voice mail, FAX services, teleconferencing, video conferencing, electronic mail, bulletin boards, list-servs, newsgroups, Internet access, web pages, traditional print information published electronically and electronic broadcasting in radio and television.

To Whom Do These Guidelines apply?
College faculty, staff, students and others affiliated with the College (including those in program, contract, or license relationships). Members of the public also may use these facilities under the caveats specified under Terms of Allowable Use in the college's "Electronic Communications Guidelines."

Protecting Sensitive Data using Electronic Communications
Protecting sensitive data is paramount for all College employees. If users occasionally send privileged or confidential data (i.e. sensitive data) electronically, they must use the following disclaimer or similar disclaimer that provides the same (or better) notification and protection of sensitive data.

Sample Disclaimer to PROTECT Electronically Sent Sensitive Data

> *"CONFIDENTIALITY NOTICE: This electronic transmission and any documents accompanying this electronic transmission are intended by College of DuPage for the use of the named addressee to which it is directed and may contain information that is privileged, or otherwise confidential. It is not intended for transmission to, or receipt by, anyone other than the named addressee or a person authorized to deliver it to the named addressee. It should not be copied or forwarded to any unauthorized persons. If you have received this electronic transmission in error, please delete it immediately, and notify the sender of the error so it can be corrected"*

Defining Data and Information Requiring Protection by the College
The College has chosen to define protected data and information to include student personal and financial information required to be protected under the Family Educational Rights and Privacy Act (FERPA), the Gramm-Leach-Bliley Act (GLBA), Children Online Privacy Protection Act (COPPA), Fair and Accurate Credit Transactions Act (FACTA), Health Insurance Portability and Accountability Act (HIPAA), and the Payment Card Industry Data Security Standard (PCI-DSS) and all future information protected by new and updated laws

and industry standards. In addition to educational records and student personal and financial information, the College has chosen to also include the personal and financial information of faculty members, staff members, alumni, and other donors in the definition of protected data and information. When in doubt as to whether a piece of data or information is to be protected, COD employees/contractors will err on the side that it is protected data and information. Protected data and information includes both paper and electronic records.

Examples of protected data and information that require protection at the College of DuPage is defined as an individual's **name** (**last name and first name or initial)**, in combination with **any** of the following data:

1. Social security number
2. Student education records
3. Driver's license number or identification card number
4. Financial account number, credit or debit card number with personal identification number such as an access code, security codes or password that would permit access to an individual's financial account.
5. Home address or e-mail address
6. Medical or health information
7. Date of birth
8. Biometric Data

Portable Media Usage Guidelines

Many College staff members use portable media, which includes but is not limited to laptops/notebooks/networks PC, smartphones, USB sticks, CDs, DVDs, and flash memory, to store and carry protected data and information. Many portable media do not provide a way to safeguard the information contained on that media. In addition, portable media is easy to lose and steal. Therefore, all College staff using portable media (which includes laptops) to transport and store College protected data and information must take the additional step to protect the data by encrypting it. Compliance with these guidelines is also required for the College to comply with Federal and State regulations, and industry standards that mandate protection of data and information that could be used for identity theft.

Portable Media Storage of Protected Data and Information

COD employees are allowed, but highly discouraged, to store protected data and information on portable media if they comply with the following requirements.

1. Must only be done for business reasons.
2. Storage of the data on the portable media must be in a security industry accepted encrypted format. The encryption process must use a current industry encryption standard to protect College protected data and information when stored on portable media. Most new USB drives have on-the-fly-encryption (OTFE) at a current industry encryption standard.

Transmission of protected Data and Information

Transmission of protected data and information is only allowed if:

1. Transmission is required for business purposes.
2. It is encrypted during transmission using a security industry accepted encrypted format. It must never be sent through unencrypted email (i.e. in plain text). Secure HTTP is the dominant encryption format for website transmission. You will know if you are using secure HTTP if you see "https://" prefixing the current URL webpage address loaded into the viewing area of your browser. For file transfer secure FTP protocols (e.g. FTPS, SFTP, or Secure FTP) are widely available and use industry accepted encryption formats for sending files securely.

What is "Allowable Use" of The College's Electronic Communications Facilities?

Those who use College electronic communication facilities must do so responsibly, i. e., comply with the public law, all College policies and guidelines and reasonable standards of professional and personal courtesy and conduct.

College electronic facilities are primarily for the use of instruction, instructional support and public service. No outside agencies or individual may use College electronic communications facilities unless their services support the College and its mission.

What is NOT "Allowable Use" of the College's Electronic Communications Facilities?
The following list is not meant to be an exhaustive list. College electronic communications facilities may not under any circumstances be used to:

- Conduct unlawful activities
- Conduct business enterprises
- Make endorsements & promotions
- Obtain personal financial gain
- Overload any technology capacities
- Violate of any other college policy
- Do anything that is inconsistent with "Allowable Use"
- Do anything with a false identity
- Interfere with the College electronic communications infrastructure
- Incur costs to the college
- Compromise the college mission
- Clash with an employee's job duties
- Send disruptive, destructive, or unproductive email
- Misrepresent the college

Email
All College employees receive a College e-mail account (@cod.edu) as a condition of employment. Accounts are created by the Information Technology (IT) department upon notification and proper authentication from Human Resources.

For students, assignment of student e-mail accounts will be created automatically for all admitted students by the Information Technology Services department after the student has created their MyACCESS account. Students are expected to check their e-mail regularly in order to stay current with College-related communications.

Email Usage Expectation
The College uses e-mail not only for dissemination of "official" information, but also for the everyday transmittal of information to ensure the smooth working of the College. E-mail's primary use is to support the business and mission of the College. The enormous growth in e-mail volume necessitates that all staff make common sense decisions about using appropriate media choice for communications. For some employee e-mail provides a ready record of all voice mail messages through an integrated messaging system. Users who use voice mail should be fully aware that such messages may be archived by the person to whom they are sent. Those who retain such messages should hold them in accordance with all other standards of use and policies governing electronic communications. The College e-mail system provides the capability of "attaching" documents and files of many media to e-mail correspondence. Such attachments are also subject to the same standards and policies as all other electronic communications.

Email Retention
If the information content of email gives rise to a level of a permanent record that must be retained in accordance with laws, regulations, and standards that currently apply to the College now and in the future (see section 5.4.1), the College employee must archive and preserve the email outside the email system for the length of time required by the applicable law, regulation, and/or standard. If an employee has questions about how they are to store the college record, they may contact the IT Helpdesk.

Social Media Guidelines
College of DuPage may utilize social media and social network sites to enhance communications with students, employees, and the community. Social media facilitates discussion of College issues, operations, and services by providing students, staff, faculty, and members of the public the opportunity to interact and participate using a variety of venues. Any official College of DuPage presence on a social media site or service is considered an extension of the College's electronic communications infrastructure and must comply with all College policies,

state and federal regulations/laws, and industry and professional standards. For a detail set of guidelines for official College of DuPage social media sites refer to the College's "Electronic Communications Guidelines."

Employees, students, alumni, and community members may also have a personal or "non-official" social media site or sites. For personal social media sites, the owner must still abide by COD guidelines that protect the College's data, goodwill, reputation, etc. For a detail set of guidelines for personal or "non-official" College of DuPage social media sites refer to the College's "Electronic Communications Guidelines."

What is My Expectation for Privacy?
Free and open communications are the hallmark of good education and the College maintains a strong commitment to academic freedom, shared governance, freedom of speech and the privacy of information with which it is entrusted. These commitments can be more complex to maintain in the world of electronic communications. Nonetheless, the College does encourage electronic communications and does not routinely inspect, monitor or disclose electronic communications.

However, because the College may deny access to electronic communication services for, but not limited to, improper use, capacity, and technology, it may inspect, monitor, or disclose electronic communications under appropriate circumstances.

College policies on maintaining the privacy of its printed and electronic records also apply to all kinds of electronic communications. However, the College cannot take responsibility for all the challenges modern electronic technologies pose to privacy. Similarly, it cannot assume responsibility for the negligence or inattention to issues of privacy that are the responsibility of users of the electronics communications systems (see "User's Privacy Responsibility" below).

What is the User's Privacy Responsibility?
Users cannot disclose their password to anyone else. Users cannot re-use a password for their College account, and users must not use their College password for any non-College account or purpose.

The College is committed to doing its best to maintain the security of its electronic communications within the bounds of the law, technical feasibility and cost. Users of these facilities bear a significant part of the responsibility for this security. Users should make careful judgments about just how secure a given mode of electronic communication is. Essentially, the more mature the means of communication, e. g. the United States Postal Service or voice telephones, the more privacy one might expect, both through technology and the body of law that has grown up around these older technologies. Newer forms of communication may be technologically less secure and may lack the buttressing laws to protect the user.

What is the Penalty for Violating the Electronic Communications Guidelines?
Both public law and College policies prohibit the theft or abuse of all its computers, other electronic software and support systems (including computers that support electronic communications facilities, systems, and services). Abuses include (but are not limited to) unauthorized entry, use, transfer, tampering with the communications and/or work of others and with other electronic communications facilities, systems, and services. Certain types of abuses constitute criminal behavior. All employees are encouraged to familiarize themselves with these laws and their relation to College policies and guidelines.

In addition to legal sanctions, violators of these guidelines may be subject to disciplinary action including dismissal or expulsion, as relevant, consistent with other College policies, procedures or collective bargaining agreements.

For more information refer to the "Electronic Communications Guidelines" and/or contact Keith Conlee, Chief Security Officer for Information Technology, SRC 2157, (630)-942-3055.

College of DuPage
425 Fawell Blvd.
Glen Ellyn, IL 60137-6599