chatham
UNIVERSITY

Cybersecurity & Data Protection at Chatham University

Information Technology Services is responsible for policies, systems, and practices that protect the University from cyber threats, maintain compliance with audit and other regulatory requirements, ensure quick and reliable backup and recovery of systems and data, and manage a complex and secure multiuser computer environment. Below is a highlight of some key policies, programs and legal requirements.

GLBA

The Gramm-Leach-Bliley Act (GLBA) is a federal law that protects personally identifiable information (PII) and applies to all entities that collect consumer financial data, including institutions of higher education. It governs how we at Chatham collect, store, and use student records containing personally identifiable information. Chatham works to maintain compliance with GLBA through procedures and policies outlined in this document.

Chatham requires mandatory annual GLBA training (June of each year) for all faculty and staff to enhance awareness of our responsibilities as employees to protect PII, even if access to PII is not normally part of our day-to-day responsibilities. A link to the 2022 training is accessible here: https://my.chatham.edu/documents/view.cfm?DocID=8611.

Data Breach Notification

Chatham University is committed to protecting the security, confidentiality, and integrity of Personal Identifiable Information (PII) of students, staff, and faculty. As part of this commitment, the University will notify affected individuals of a data security breach as required by the relevant local, state, or federal laws. PII may include, but is not limited to:

- An individual's name (first name or first initial and last name), or phone number, or address, in conjunction with any of the following data elements:
    - social security number
    - credit and debit card information
    - income and credit history
    - bank account information
    - driver's license number
    - tax return
    - asset statement
- Any number or code or combination of numbers or codes, such as account number, security code, access code, or password, that allows access to or use of an individual's financial or credit account.
- Covered Information includes both paper and electronic records.

The following safeguards must be implemented by offices which maintain or handle covered information:

- Require all employees to immediately notify their supervisor of any actual or suspected security breach involving files containing PII. If employees are uncertain whether there has been a breach, they must report the event to their supervisor.

If a data breach has occurred or is suspected, supervisors must immediately report the event to the Chief Information Officer. An evaluation regarding whether there has been a data breach of Personal Information requiring notification to affected individuals will be conducted.

Electronic Discovery
During a civil lawsuit, any potentially relevant evidence may be subject to discovery, even if that evidence is not admissible at trial. Electronically Stored Information (ESI) is essentially any electronic information that could serve as evidence in civil litigation. Local hard drives, e-mail, shared storage, backup systems, mobile devices (e.g., cell phones, PDAs, etc.) and removable media (e.g., CDs, DVDs, flash drives, etc.) are all potential sources of ESI.

When civil litigation is reasonably anticipated, Chatham University will preserve historical and prospective ESI from destruction. In addition, Chatham may be required to:

- Provide a description by category and location of all ESI in its control which may be relevant to the case.
- Produce ESI in original format if it is relevant, not privileged and reasonably accessible.

GDPR
Information related to the European Union's General Data Protection Regulation (GDPR) and the ability for users to opt-out of cookies via Cookie Control is available on Chatham's website and Privacy Policy web page here.

Cybersecurity Training
Chatham enhances overall cybersecurity defenses, while also working to support good cybersecurity practices among employees and students through annual cybersecurity training. This training increases knowledge and practices and helps users avoid scams, malicious links, and protect personal data. This training was launched in March 2023 and will be conducted annually, each academic year.

Employee Use of the University's Communications Systems, Business Equipment and Supplies
The University's communications systems, as described below, including but not limited to, Internet, email, telephone, facsimile, photocopiers, printers, office equipment and supplies, are intended for University business purposes. Any necessary use of these systems for personal purposes should be kept to a minimum and be done in accordance with the University policies outlined below.

Employer Rights Regarding Employee Use of University Communications Systems

The University reserves the right to monitor, access, search, block, copy, delete, review and disclose at any time messages or documents created, sent, stored or received on, as well as any websites visited on, any of the University's communication systems, whether accessed on site or via remote locations, including, but not limited to:

- Telephone systems
- Fax machines
- Computer software/applications and hardware
- Workstations, Desktops, and Laptops
- Remote Access servers and applications
- Network/File servers
- Email servers and systems
- Instant messaging networks
- Text messaging networks
- Voicemail systems
- Internet Servers
- Portable devices, such as PDAs, pagers, USB drives, iPhone, iPad, tablet devices, slate computers, memory sticks, flash drives, CDs, DVDs, cell phones and palm pilots or other smart phones

By using the University's communications systems with respect to which you have no expectation of privacy, whether accessed on site or via remote locations, employees consent to the University's monitoring, accessing, searching, blocking, copying, deleting, reviewing and disclosing, both real time and after the fact, any documents or messages which they create, send, store or receive on, as well as websites visited on, the University's communications systems.

The University contracts with certain third-party service provides (for example, electronic communication service providers and/or remote computing service providers) to deliver and store certain communications which are sent or received on the University's communications systems, including, by way of example only, instant messages, text messages and email.

By using the University's communications systems with respect to which you have no expectation of privacy, whether accessed on the University's premises or via remote locations, employees consent to the University's third-party service providers monitoring, accessing, searching, blocking, copying, deleting, reviewing and disclosing to the University, both real time and after the fact, any documents or messages which employees create, send, store or receive on the University's communications systems but which also may be received and stored by one of the University's third party service providers, including any electronic communication service provider or a remote computing service provider.

Any theft of, tampering with, or other destruction of computers, software programs and network services is prohibited.

Failure to cooperate with the University in its exercise of any rights described in this Policy is cause for an employee's immediate discharge. In addition, any employee who engages in conduct intended to interfere with or prevent the University from exercising any of its rights as described in this Policy will be disciplined, up to and including termination.

Internet Use

This Internet Use policy applies to desktop computers, laptops, as well as electronic hand-held devices, such as iPads, tablets/slate computers, and smart phones.

1. Permitted Purposes

Generally speaking, employees may access the Internet through the University network or using University-provided equipment solely for the purpose of conducting business for the University. However, the University's network and/or equipment may be used for non-business purposes if such non-business use is kept to a minimum (for example, quickly checking the weather, the news, or the stock market) and such non-business use does not interfere in any way with business activities or otherwise violate this Policy.

During non-working time, such as breaks, employees may access the Internet for personal purposes so long as they do not access sexually-explicit or –suggestive Internet sites or other sites that are inconsistent with our EEO policy, for example, sites that disparage or stereotype any age, race religion, etc.

Further, any expenses incurred by the employee with regard to non-business use must be paid by the employee.

Finally, at all times, employees must follow all applicable laws, regulations and other University policies when accessing the Internet.

1. Copyrights and Downloads

Employees must obtain written approval from their supervisor before downloading any materials for which an online (or "click") agreement must be completed.

Employees shall refrain from illegally copying any works or making available copies of any works that are protected by copyright, including, but not limited to, software, music and videos. Employees are responsible for observing copyright and licensing agreements that may apply when downloading files, documents and software. Under no circumstances shall an employee purchase, copy or install any software on University equipment without the prior written approval of the supervisor and Chief Information Officer.

2. Prohibited Uses

Employees are prohibited from sending or posting any type of communications over the Chatham network that defame or libel our students, threaten to cause property damage or physical harm to any person, including but not limited to our employees, students, or others with whom Chatham does or may do business.

Further, employees must guard against the disclosure of confidential information through the use of Internet, e-mail or otherwise through the use of Chatham's communications systems. If transmitting confidential information for a permissible purpose, employees must ensure that they are doing so consistent with Chatham policy and applicable law, including but not limited to protecting the privacy of student education records under FERPA.

Employees shall not view, download, copy, send, post or access information that is illegal, obscene or otherwise inconsistent with the University's non-discrimination and non-harassment policies (e.g., sexual images, sexist comments, racist messages, ethnic slurs, religious slurs).

3. Monitoring

As an additional reminder which is set forth more fully in the section on Employer Rights Regarding Employee Use of University Communications Systems, employees have no right to privacy with respect to use of Chatham's communications systems, whether accessed on site or via remote locations including but not limited to Internet searches and communications involving the University's Internet server, and consent to the University's monitoring, accessing, searching, blocking, copying, deleting, reviewing and disclosing of their Internet searches and communications, both real time and after the fact.

2. University Network Security

Employees shall access the Internet in a manner which does not compromise the security and integrity of the University network such as allowing intruders or viruses onto the University network. Employees wishing to download any document, file or software from non-University sources must observe University policies and procedures for virus checking and system security.

A user's network account may be temporarily suspended, be reduced to an appropriate level, or blocked, when necessary to do so in order to protect the integrity, security, and functionality of University technology resources, or to protect the University from liability.

Access to University technology resources may be removed immediately. Reasons for removal may include, but are not limited to, the following: the individual is terminated for cause and there is concern for safety of systems or data; there is reasonable belief that the individual to whom the account is assigned has perpetrated or is involved in illegal activities or activities that violate University policy.

Any violations of this policy are cause for discipline, up to and including discharge.

Email Communications

Please keep in mind that this policy applies to email use by way of desktop computers as well as by way of electronic hand-held devices, such as iPads, tablets/slate computers, and smart phones whether University-issued or personal that are used to conduct University business.

The Chatham University email system provides a quick and efficient way for employee communication. Although email is designed for business purposes, the University recognizes that some personal use of email may occur. These non-business uses should be kept to a minimum and not interfere with business activities. During non-working time, such as breaks, employees may use e-mail for personal purposes so long as they do not violate this policy or any other University policy, for example, even during non-working time, an employee cannot use the University's e-mail to send a sexist, racist or ethnic "joke" or slur.

When sending a personal e-mail, please be careful not to state or suggest that you are speaking on behalf of the University or that your views reflect those of the University.

It bears repeating that the University's Code of Ethical Professional Conduct and Policy on Equal Opportunity applies to email communications. In particular, and by way of example only, you should neither send nor forward any emails which are sexual or suggestive or which stereotype, disparage or otherwise make fun of any protected group, for example, any race, religion, ethnic group, gender, sexual orientation, age, or disability.

As set forth more fully in the section on Employer Rights Regarding Employee Use of University Communications Systems, because the email system is the property of the University with respect to which you have no expectation of privacy, the University reserves the right to monitor, access, search, block, copy, delete, review and disclose messages created, sent, received or stored on the email system or through/on one of the University's third party service providers, including any electronic communication service provider or remote computing service provider. By using the University's email system (whether on a wired or wireless device), you consent to the University's monitoring, accessing, searching, blocking, copying, deleting, reviewing and disclosing messages, both real time and after the fact, that you create, send, receive, or store on the University's email system or through/on one of the University's third party service providers, including any electronic communication service provider or remote computing service provider.

While there are email backups for erased email messages, the backups are not retained indefinitely. Accordingly, if a communication should be preserved, you can archive it in accordance with IT guidelines and/or print it out for paper filing. If you have any question as to whether and how to preserve an email, please contact the ITS (Information Technology Services) Support Services (Helpdesk) on ext. 1112.

An employee who violates the Policy will be subject to appropriate disciplinary action, up to and including immediate discharge.

Computer Policy

Licensing agreements and other legal restrictions and requirements apply to the use of computers (including laptops, iPads, Smartphones, tablets/slate computers), software programs and network services. Information Technology Services is responsible for ensuring the University's compliance with these licensing agreements and other legal restrictions and requirements.

To ensure legal compliance and to avoid the inadvertent creation of technological problems, an employee must obtain prior approval from their supervisor (or an Officer of the University who has consulted with the Chief Information Officer) before he or she:

- Copies University-provided software programs (even if from one University computer to another or to a storage device such as a USB flash drive or external hard drive).
- Installs or loads on or downloads or removes from a University computer or from any network service any software programs or other electronic content (including, but not limited to, games, screen savers, digital photographs or video, anti-virus software and shareware or freeware).
- Installs University-provided software programs on a home or other non-University computer system.
- Installs new hardware on University computers or attempts to service University computers or any other computer peripherals.
- Upgrades, enhances or attempts to alter or reverse engineer any software program.

An employee who engages in any of the activities set forth above without the prior approval required by this Policy, or who violates the guidelines provided by the Information Technology Services Department where approval has been granted, will be subject to appropriate disciplinary action, up to and including discharge. No devices can be attached to the University network unless it has updated antivirus, malware, and operating system patches installed.

Passwords are provided to all students and employees who have access to the University's computers. An employee may neither use another employee's or student's password nor permit another employee or non-employee to use his or her password to access the University's computer systems.

As set forth more fully in the section on Employer Rights Regarding Employee Use of University Communications Systems, because the University's computers and storage devices (including cloud storage such as OneDrive, flash drives, external hard drives, tapes, DVDs and CDs) are the sole property of the University with respect to which you have no expectation of privacy, they and any information you create or store on them are subject to search and monitoring by the University at any time at the University's sole discretion. Similarly, any University-provided software program authorized for use by an employee on his or her home computer system or elsewhere subjects any such computer system (with respect to which you have no expectation of privacy) to search and monitoring by the University at any time in its sole discretion.