Grayson College
Acceptable Use Policy

History

Version No.	Issue Date	Status	Reason for Change
v1.0	10/15/2020	Draft	

Review

Reviewer's Details	Version No.	Date

1. POLICY

It is the policy of the Grayson College that the use of the College's Computer Resources shall be mainly used for college purposes that support the school's mission. Computer Resources refers to Grayson College's entire computing network and technology infrastructure. This includes: host computers, file servers, application servers, communication servers, mail servers, web servers, workstations, stand-alone machines, laptops, mobile computing devices, software, data files, and all internal and external computer and communications networks (i.e. Internet, commercial online services, value-added networks, e-mail systems, etc.), and any technology that enables or supports college activities, that may be accessed directly or indirectly from our internal network, and may change from time to time.

Grayson College relies heavily upon its technology assets to conduct operations. As such, the availability and integrity of these systems are critical to the delivery of services that we offer our stake holders, as well as the broader college community. Recognizing this, Grayson College has created a policy which guides the proper use of these assets, while being careful not to impose restrictions contrary to Grayson College's established culture of openness, trust, and integrity.

The purpose of this policy is to set forth Grayson College's expectations and requirements regarding the acceptable use of College Computer Resources.

2. SCOPE

This policy applies to employees, students, and representatives of Grayson College who use Company Computer Resources (individually each a "User," collectively, Users"). A "User" includes consultants, contingent workers, and temporary employees. Any Grayson College user who is given access to College Computer Resources should also adhere to this policy concerning those resources. Grayson College's communication systems are intended for use primarily in conducting college operations.

Nothing in this Policy is intended to prohibit users from engaging in communications protected by federal state and/or local law, including but not limited to, communication related to hours, wages, or other terms and conditions of employment, or to affect employees' rights to report matters to governmental authorities in accordance with applicable law.

3. POLICY STATEMENT

Under the provisions of the Information Resources Management Act (Texas Government Code, Title 10, Subtitle B, chapter 2054), information technology resources are strategic assets of the State of Texas that must be managed as valuable state resources.

Grayson College provides electronic communication services to faculty, staff and students, and to other affiliated classes of individuals, including retirees and official visitors. Use of Grayson electronic communication services must be consistent with Grayson's educational goals and comply with local, state and federal laws and College policies.

Communications via Grayson electronic systems are the property of Grayson, and management maintains the right to access when necessary. All user activity on Grayson information technology resource assets is subject to logging, review and open records.

All electronic communication activities must comply with this Acceptable Use Policy

The following activities are expressly prohibited as specified by Texas Department of Information Resources in response to TAC §202 requirements:

- Sending electronic communication that is intimidating or harassing.
- Using electronic communication to transmit or receive material that may be offensive, indecent, or obscene.
- Using electronic communication for conducting personal business.
- Using electronic communication for purposes of political lobbying or campaigning.

- Violating copyright laws by inappropriately distributing protected works.
- Posing as anyone other than oneself when sending electronic communication, except when authorized to send messages for another when serving in an administrative support role.
- Sending or forwarding chain letters.
- Sending unsolicited messages to large groups except as required to conduct College business.
- Sending messages with excessively large attachments.
- Sending or forwarding electronic communication that is likely to contain computer viruses.
- All sensitive Grayson material or email containing sensitive data transmitted over external network must be secured during transmission.
- Electronic communication users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of GC or any unit of GC unless appropriately authorized (explicitly or implicitly) to do so. Where appropriate, an explicit disclaimer will be included unless it is clear from the context that the author is not representing GC. An example of a simple disclaimer is: "the opinions expressed are my own, and not necessarily those of my employer."

4. REQUIREMENTS

A. EXPECTATION OF PRIVACY

Users shall have no expectation of privacy while using Grayson College Computer Resources.

Users expressly waive any right to privacy in anything they create, store, send, or receive on Grayson College Computer Resources. Users consent to allowing personnel of Grayson College to access and review all materials they create, store, transmit or receive on or through any Grayson College Computer Resources.

Users understand that Grayson College will routinely use human or automated means to monitor the use of its Computer Resources and may access, retrieve, and delete any material.

B. GENERAL SYSTEM USAGE

Grayson College, at its discretion, provides Users access to its Computer Resources. All Users accessing Grayson College Computer Resources should use these resources primarily for the purposes for which they are employed or engaged and agree to comply with this Policy.

Computer Resources Grayson College provides are considered College property. Usage of Grayson College Computer Resources is subject to monitoring by Grayson College to ensure compliance with this and/or other policies.

It is understood that incidental personal use of Computer Resources such as email, telephone, and the Internet may occur during non-working time. When using Grayson College Computer Resources, Users are expected to exercise sound judgment, refrain from personal use during working time, and avoid sending any material in violation of Grayson College written policies or any and all laws. Though recognized, such use should never interfere with a User completing their assigned duties and must be limited to non-working time. Every User must use Grayson College Computer Resources responsibly, ethically, and lawfully.

While recognizing the existence of instances of personal use, Grayson College does not imply a right to privacy. All personal use of Grayson College's systems is subject to monitoring.

Users will not permit and make reasonable efforts to prevent, unauthorized persons to access or use Grayson College Computer Resources.
All Grayson College data and information accessed or processed through its Computer Resources should be managed in adherence to its sensitivity and information classification, as outlined in the Grayson College Written Information Security Program.

Grayson College's information shall not be stored on personal devices; except for authorized mobile devices and removable media. Using a personal mobile device to receive Grayson College email where approved; Users must agree to follow this Acceptable Use Policy and allow Grayson College to perform a remote wipe on the device if lost or the User leaves Grayson College. In addition, personally owned computers and/or mobile/smart devices used for business purposes may become subject to legal hold for evidence requirements and possible confiscation in case of an investigation.

C. EMAIL, MESSAGING, CHAT, and TEXT USAGE

All Incoming email should be treated with the utmost care due to its inherent information security risks. An email with file attachments received from unknown or unexpected sources should not be opened unless the identity of the sender has been verified.

Emails and their attachments should be managed in accordance with established Grayson College information classification requirements. Personal and Restricted business information should only be emailed outside of the college in accordance with relevant Grayson College policies and statutory requirements. The use of encryption does not negate these obligations. Confidential information that must be emailed outside of the organization must be encrypted.

Use of Grayson College Computer Resources must follow all Grayson College policies. Never use Grayson College email to set up personal businesses or to send “spam,” create or participate in “pyramid schemes,” or conduct any illegal activity.

To prevent Grayson College’s waiver of the attorney/client privilege, when corresponding on behalf of Grayson College on legal matters affecting Grayson College, any messages to or from legal counsel should not be forwarded or distributed to others without first consulting with legal counsel.

Information forwarded by email (especially attachments) should be correctly addressed and only sent to intended recipients. Users should not send/email/transfer communications made as a part of job duties to or from personal email accounts or messaging platforms, video conferencing/chat services, texting, or other means not approved by Grayson College for use. Grayson College’s email system is intended for use in conducting college related business and operations.

All emails sent to external destinations will automatically contain the standard Grayson College email disclaimer.

“The information contained in this e-mail and any accompanying documents is confidential, may be privileged, and is intended solely for the person and/or entity to whom it is addressed (i.e., those identified in the "To" and "cc" box). They are the property of Grayson College. Unauthorized review, use, disclosure, or copying of this communication, or any part thereof, is strictly prohibited and may be unlawful. If you have received this e-mail in error, please return the e-mail and attachments to the sender and delete the e-mail and attachments and any copy from your system. Grayson College appreciates you for your cooperation.”

Only messaging systems approved by Grayson College should be used on college equipment. Messaging should not be used to transmit information, including attachments, having long-term business value.

D. INTERNET/INTRANET USAGE

Grayson College is not responsible for any content or materials made available over the Internet by third parties, including without limitation any electronic mail transmissions, newsgroups, weblogs or similar technologies. Grayson College may remove, block, filter, or restrict by any other means any materials that in Grayson College's sole discretion it believes may be illegal, may subject the college to liability, or may violate this policy. Grayson College may cooperate with legal authorities and/or third parties in the investigation of any suspected or alleged crime or civil wrong associated with the use of Grayson College Computer Resources.

Only communications explicitly authorized through Grayson College communications or marketing should be published on social media sites on behalf of Grayson College.

A User's ability to connect to other computer systems does not imply a right to connect to those systems or to make use of those systems unless authorized explicitly by Grayson College and the operators of those systems.

Users may not use Grayson College systems and Internet access to access, upload, publish, or download material from the Internet which is illegal under local, state, federal, or international law, jeopardizes system availability or security or violates any Grayson College established policy. Examples of prohibited usage include, but are not limited to:

1. Violating the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including but not limited to the installation of "pirated" or other software products that are not appropriately licensed for use by Grayson College.
2. The exporting of software, technical information, encryption software or any technology in violation of international or regional export control laws.
3. Intentionally or maliciously introducing malicious programs into any network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).
4. Effecting security breaches or disruptions of network communications (e.g., network sniffing, ping floods, packet spoofing, denial of service, and forged routing information).
5. Procuring or transmitting material that is in violation of applicable laws or Company policies prohibiting sexual harassment and/or a hostile work environment.
6. Monopolizing Company resources (e.g., sending large attachments, such as videos, or otherwise creating any unnecessary burden on the network).
7. Due diligence should be taken when downloading information

and files from the Internet to safeguard against both malicious code and inappropriate material (e.g., pornography).

8. Grayson College information should only be stored on approved servers. The use of public/cloud data centers (e.g., DropBox, Apple iCloud, Google Docs, etc.) is prohibited.
9. There should be no Peer to Peer (P2P) or Virtual Network Computing (VNC) protocols running and using network traffic.

E. TELEPHONE/FAX USAGE

Information classified as Grayson College Confidential should not be: (i) recorded on answering machine/voice mail systems; or (ii) provided over the telephone unless the recipient's identity has been verified and that person is authorized to receive such information.

Information classified as Grayson College Confidential may only be faxed where more secure methods of transmission are not feasible. Both the owners of the information and the intended recipient are required to authorize the transmission beforehand.

F. PASSWORD REQUIREMENTS

All Grayson College users must select a unique passphrase or passwords following these guidelines:

1. Is at least 10 characters long;
2. Contains a combination of uppercase and lowercase letters, numbers, and special characters (i.e. @, !, *);
3. Does not include repeated characters or a sequence of keyboard strokes (i.e. 1234, mmm888, or asdfg); and
4. Does not include any part of the user's name, birthday, or other personally identifiable information, or that of friends and family.
5. Shall be changed at least every 90 days, or as necessary.

G. MOBILE DEVICES AND REMOVABLE MEDIA USAGE

Mobile/smart devices and removable media should be secured with a complex password if used to access or store Grayson College information per the Grayson College Information Security Program.

Software applications must only be acquired from platform native application stores such as Windows Store, iOS App Store, Android Google Play. Downloading from secondary app stores is prohibited.

Mobile/smart devices and removable media should only be used for the storage of Grayson College information in accordance with the requirements for the storage and disposal of Grayson College information, as defined in the Grayson College Written Information Security Program.

Removable media should be checked for malicious code upon connecting to Grayson College -owned systems.

Users are responsible for the security of Grayson College Computer Resources in their custody (whether traveling, working remotely, or in College offices) and should protect the equipment and information from unauthorized access, misuse, corruption, physical damage and/or loss.

.

Personnel issued mobile devices by Grayson College are responsible for using them in a manner consistent with the confidentiality level of the information being accessed or discussed, as defined in the Grayson College Written Information Security Program.

H. SOFTWARE USAGE, COPYRIGHT COMPLIANCE

All software installed and/or used on Grayson College computers must be owned by and/or covered by a valid license agreement and approved by IT. Installation and use should be in accordance with the terms and conditions set out in the applicable license agreement. Grayson College’s IT department is exclusively responsible for installing and supporting all software and hardware used for Grayson College operations.

Grayson College and third-party software, including written materials such as manuals, should not be removed from or copied outside of Grayson College’s premises except as expressly approved by IT. All software may only be used in the manner that Grayson College and the software vendor intended. Do not incorporate third-party software, including written materials such as manuals into Grayson College software in performing your work unless expressly permitted to do so by any applicable agreement under which the software was acquired.

Any use of open source software should comply with the requirements listed in the Grayson College Written Information Security Program, including understanding the license full terms and conditions, having the license reviewed by Legal Counsel, having a College employee request the open source software, and maintaining compliance with the software’s statement of use requirements

I. NETWORK CONNECTIVITY

Using public computers at hotel business centers, Internet cafes, public kiosks or elsewhere to log into the Grayson College network and systems is strictly prohibited. When using a Grayson College issued laptop on a public network (i.e., internet cafe, library, hotel business center), Users must access Grayson College resources via an approved VPN solution. Third Party VPN connectivity into the Grayson College network requires approval from IT. A security evaluation of any third-party connection may be required.

Users may only use approved file transfer methods when sending Company information to parties outside of the Grayson College network in adherence with the Grayson College Written Information Security Program. Users are not allowed to attach networking equipment (e.g., hubs, switches, and wireless communications devices) to the network unless it is approved and configured by Grayson College IT.

J. COMPUTER SYSTEM SECURITY MEASURES

Grayson College shall maintain up-to-date operating systems and security patches for systems or services. Grayson College shall also provide up-to-date versions of licensed system security agent software, including anti-virus and malware protection, together with up-to-date patches and virus/malware definitions.

Grayson College will install firewall software on all portable and remote devices that store ePHI/PHI, PII, SPI, and other Data or connect to networks on which such is accessible. All portable or remote devices that store ePHI/PHI, PII, SPI, and other Data will employ the highest currently available encryption technologies, use passwords/passphrases, and wherever available multi-factor authentication (MFA) technology will be employed.

Licensed system-wide security agent software, which includes malware protection, patches, and virus definitions, is installed on all Grayson College systems. This software will be updated daily automatically (and manually when needed) on all systems.

All Grayson College computer systems will be monitored persistently for unauthorized use of or access. Any unauthorized use or access found will be immediately reported to the Information Security Officer. Further, actions will be taken to assess the impact of the unauthorized use/access, appropriate measures will be taken against employees not complying with this WISP, and updates will be made to the safeguards specified in this WISP as needed to prevent future unauthorized access/use of ePHI/PHI, PII, SPI, and other Data

5. TRAINING

This Acceptable Use Policy shall be provided to each of Grayson College ’s employees who has access to systems, or processes Data owned or controlled by Grayson College. Each such individual is also required to complete a training program on information security and this Acceptable Use Policy. The Information Security Officer shall be responsible for introducing the AUP to new employees as part of Grayson College onboarding process.

6. DISCIPLINE FOR VIOLATION OF THE PROGRAM

Consistent with Grayson College policies, the ISO is authorized by the Grayson College President to ensure that the appropriate processes to administer this program are in place, communicated to, and followed by the college community.

Administrators must ensure that measures are taken within their department to comply with this policy and its related standards, guidelines and practices. Departments found to be non-compliant will be required to take specific steps to come into compliance within a specified time. If compliance cannot be achieved, a written request for exception must be approved by the ISO. Approved requests will be reviewed annually to determine if an exception is still warranted.

Grayson College reserves the right to temporarily or permanently suspend, block, or restrict access to college information technology resources, independent of such procedures, when it reasonably appears necessary to do so in order to protect the confidentiality, integrity, availability or functionality of Grayson College information technology resources; to protect Grayson College from liability; or to enforce this policy and its related standards and practices.

Failure to adhere to the provisions of this policy statement or the appropriate use policy statement may result in:

- ·Suspension or loss of access to Grayson College information technology resources
- ·Appropriate disciplinary action under existing procedures applicable to students, faculty and staff, and
- ·Civil or criminal prosecution

Potential violations will be investigated in a manner consistent with applicable laws and regulations, and Grayson College policies, standards, guidelines and practices (TAC§202.72) (TAC§202.73).

The Vice President for Administrative Services or designee will ensure that suspected violations and resultant actions receive the proper and immediate attention of the appropriate college officials, law enforcement, outside agencies, and disciplinary/grievance processes in accordance with due process.

Third-party service providers who do not comply may be subject to appropriate actions as defined in contractual agreements or other legal remedies available to Grayson College.

Appeals of college actions resulting from enforcement of this policy will be handled through existing disciplinary/grievance processes for Grayson College students and employees.

14. POLICIES CROSS-REFERENCED

The following Grayson College policies provide advice and guidance that relates to this Program:

A. Grayson College Written Information Security Program
.