WEBB INSTITUTE INFORMATION TECHNOLOGY POLICY

It is the intent of Webb Institute (Webb) to provide a quality technological environment for the college community in which certain standards are observed. All Webb Institute students, faculty, and staff authorized to use Webb Institute computing facilities are responsible for reading, understanding, and complying with the following policies.

Webb Institute provides computing and networking resources to students, faculty, and staff for various purposes. The purpose of the Webb Institute network is to support education, communication, and research by providing access to unique resources and the opportunity for interaction and collaborative work through the Internet, email, and other applications. These resources, networked for the general benefit of the community, are continually updated and maintained by the Department of Information Technology (IT Department) to provide an environment that is consistent with the educational goals of the college. These resources are limited, and how everyone uses them may impact the work of other members of the community and beyond, as our campus network is connected (through the Internet) to other networks worldwide. It is important that everyone is aware of his or her individual obligations and what constitutes proper use and behavior.

Use of Webb-owned computers and the campus network and other communications systems is considered a privilege, not a right. Webb Institute reserves the right to limit, restrict, or extend computing/networking privileges and access to computer resources. Electronic communications, including electronic mail, mailboxes, Internet, and the contents, (subject to the intellectual property policies of Webb Institute) created or stored on any Webb computer or network-related equipment, are the sole property of Webb Institute. Computers and the campus network are provided to assist students and staff in the completion of their academic pursuits and job duties and to support Webb's daily operations and long-term goals. Webb Institute reserves the right to monitor computer/network activity and communications, including Internet access at its discretion for legitimate business and educational purposes. Notwithstanding the Institute's right to preserve, access, and disclose a user's electronic information, out of respect for personal privacy, Webb does not routinely examine the contents of data or files in user accounts. However, circumstances may require an examination of a user's files to maintain system security, to administer or maintain system integrity, or in response to a legal mandate. In such cases, authorized personnel may examine a user's data without notice to the user. Authorized personnel are those specifically entrusted and approved in writing to conduct such examinations by the President.

The technology resources are maintained to enable the Webb related work of students, faculty, administration, and staff. Appropriate uses include instructional use in Webb classes, class assignments, and faculty and student research. Personal use by authorized users that does not interrupt or diminish access to resources for other users or violate the policies in the employee and student organization handbooks is permitted.

Support Provided by Webb's IT Department

The IT Department is committed to supporting Webb furnished computers and other devices and maintaining the network and related services. To do so, the full cooperation of all users is required. The IT Department will only support:

- Software that has been purchased by Webb Institute in support of Webb related work.
- The software which is installed on supported operating systems.
- Hard drive partitions as configured by the computer's manufacturer or the IT Department.
- BIOS settings without passwords. Please disable BIOS passwords before requesting support.
- If enabled, please disable Biometric passwords before bringing your laptop to support.
- Electronic communication that supports instruction, research, or official work of students, faculty, administration, and staff.
- POP3, for users who wish to download email on a single computer.

User Responsibilities

To assist in maintaining security and reliability of the network, users are responsible for:

- Keeping the preinstalled Antivirus on your mobile workstation. Removal of the Antivirus will be a violation of the Webb Security policy
- Users are responsible for basic maintenance of their systems such as keeping Windows up to date and firmware updated.
- The latest Windows updates and firmware are required to be installed on user systems prior to contacting the IT Dept for support. The only exception would be if the system is unbootable.
- Maintaining the security of all their accounts and passwords.
- Ensuring that they are using the most up-to-date virus data files. All personal- owned computers and other devices that can access the Webb network must have anti-virus software installed that is updated regularly. Virus-scanning software licensed by Webb Institute is available for all student, faculty, and staff computers. Any computer or network device that is found to be infected will be removed from the campus network until anti-virus software is installed and used to clean the computer of all viruses and malware.

Encrypted email must be used when it includes

- Social security numbers, both full and truncated.
- Driver's license and other government identification numbers.
- Financial Information such as bank account, credit, & debit card numbers
- Medical Information
- Login Information
- Grades
- Attaching any kind of sensitive document to an email
- Any recognizable format of sensitive information

General emails should not be encrypted

To update this list please contact the Director of Information Technology for approval Violation of this policy will be reviewed by the President on a case-by-case basis

Unacceptable Uses of Webb's Technology Resources

Violating one or more of the unacceptable use policies may result in the system being blocked from accessing the Webb IT infrastructure. Should the violation be of an urgent matter no advanced notice will be given to protect the security of the Webb network and its connected users. Access can be restored by written notice from Webb's President to the IT Dept.

- Violating software copyright laws. Computer software must be used in accordance with license agreements, whether it is licensed to Webb Institute or to an individual user. Transmission of unlicensed software over the campus network is prohibited.
- Violating Federal Copyright Law by downloading copyrighted audio, video, graphics, or text materials from the Internet without proof of proper licensing arrangements. Further information on the Digital Millennium Copyright Act of 1998 may be found at www.loc.gov/copyright/legislation/dmca.pdf
- Copying, publishing, storing, or transmitting data when doing so would constitute a violation of copyright.
- Using of another person's account or giving your password to allow another person to gain access to a Webb-owned computer, network, or database resource. This includes, but is not limited to, unauthorized use of an account, use of an account for a purpose for which it was not intended, or use of another person's email address.
- Accessing a file on the Webb Campus Network without the permission of the owner to copy, rename, modify, examine, or change file protection or visibility. **Lack of protection on a file does not imply right of access**.
- Introducing data or programs which in some way endangers computing resources or the information of other users (e.g., computer worm, virus, malware, or other destructive programs), or which infringes upon the rights of other Webb Institute users (e.g., inappropriate, obscene, pornographic, bigoted, or abusive materials) is prohibited.
- Running of programs that are wasteful of system resources that noticeably reduces the performance of the system for other users is prohibited. Users must recognize that computers and networks are a limited resource.

- Abusing or mistreating computing equipment. All users should become thoroughly familiar with the proper operating procedure for a given device before attempting to use it. Printers, plotters, multimedia equipment, scanners, and similar equipment are quite delicate and easily damaged through careless or rough use. A user will be held responsible for any damage to equipment caused by their own carelessness.
- Circumventing logon or other security measures.
- Sending any fraudulent electronic communication.
- Using electronic communications to harass or threaten users in such a way as to create an atmosphere that unreasonably interferes with the education or the employment experience. Similarly, electronic communications shall not be used to harass or threaten other information recipients, in addition to Webb Institute users.
- Using electronic communications to disclose proprietary information without the explicit permission of the owner.
- Using electronic means to steal another individual's works, or otherwise misrepresent one's own work.
- Using of the campus network to access, download, print, store, forward, transmit or distribute obscene material.
- Creating a website on the campus network without prior permission from the IT Department.
- Violating any state or federal law or regulation in connection with use of any information system.
- Using Webb's resources including the information technology infrastructure for commercial use is prohibited. This includes cryptocurrency mining which is power intensive and deemed by Webb a commercial use. Crypto mining is also a fire hazard as it is common for the rigs to overheat. Neither personal nor Webb equipment fed by Webb power sources may be used for crypto mining.

Wireless Internet Access

- An unsecured Wireless access point (WAP) on campus represents a network vulnerability. The IT department is solely responsible for installing, authorizing, and maintaining wireless access and wireless networking services on the campus network. No other WAP's or wireless hotspot devices are permitted to be connected to the campus network. Unauthorized WAP's or wireless hotspot devices will be removed from Webb's network upon discovery and without notice. The owner of the unauthorized WAP will be considered to have violated the Computer Acceptable Use Policy and reported to the President.

Printing

- Webb institute is a green community. The default option for all print jobs shall be black & white and duplexed (both sides of the paper). Color and single-sided prints should be printed only when necessary.

Couch Computer Lab Management

- Users must obey all posted rules (*e.g.*, moving equipment is not permitted at any time for any reason). All users must follow this policy. The computers in the lab will be maintained with a standardized image for easy restoration of systems in the event of a failure. Systems will be reformatted and reinstalled or re-imaged at the end of each semester.
- Computers in the lab may be erased and re-imaged multiple times during each semester. Therefore, lab users should have no expectation of data retention on individual systems between uses. Notice of this practice will be clearly posted as a reminder to not save important files on local hard drives of any lab computer.

Personally, Owned Computer Equipment Policy

- Personally, owned computer equipment is any computer related device that was not purchased by Webb Institute. Employees must follow Webb Institute's computer usage policies when operating personally owned computing equipment while connected to the campus network.
- The IT Department is unable to provide general hardware and software support for personally owned computing equipment, regardless of the physical location of that equipment. The IT Department is not responsible for backing up any data stored on personally owned computing equipment.

Operating Systems

- Under no circumstances will a preview or beta operating system be supported.
- Newly released operating systems will not be supported until approved by the IT Department.
- Any operating system no longer supported by the software manufacturer or unable to receive the latest security updates or patches will not be permitted on the campus network. A list of approved operating systems can be obtained from the IT Department.

Remote Access Policy

- All Computers and devices that are connected to Webb Institute's internal networks via remote access technologies must meet the requirements of Webb-owned equipment. This includes personal computers.
- At no time should any Webb Institute authorized user provide their login or email password to anyone.

Faculty Consulting

- Faculty are permitted to use academic software for consulting work only if permission is first received by the software manufacturer.
- Permission should be provided in writing and a copy provided to the Director of Information Technology to be included in the software's license file.
- The IT Dept distributes mobile workstations to full-time faculty members. Adjunct professors are required to use their systems

Policy on Mobile Devices
Purpose and Scope

The purpose of this policy is to establish a framework for consistent decision-making regarding the provision of essential, business-related mobile devices to Webb Institute faculty and staff.

Policy

Eligibility to Receive a Webb-Owned Device

- The nature of the employee's job requires that Webb Institute be able to contact the employee, via voice or access to other communication/connectivity needs such as text, email, mobile applications, or data for work-related matters, OR
- The nature of the employee's job requires that the employee be accessible to co-workers for work-related matters either:
- When the employee is away from the employee's office, OR
- Outside of the employee's normal work hours.

Employee Responsibility

- As with any device that has the capability to store data, or access data via the Webb campus network or the Internet, it is the employee's responsibility to:
- Adhere to Webb Institute's data security policies
- Maintain a current backup of the device to prevent the possible loss of data
- Use campus password policy and standards
- Use policy on appropriate use of computer and network resources
- Use procedures supporting the policy on mobile devices

International Usage of Mobile Devices

Prices for international use of mobile devices with our standard plan are very high. In general, you should not carry your mobile device during international travel. If you are traveling internationally and foresee a need to use your Webb-supplied mobile device, you must initiate the following process to avoid personal liability for international device charges:

- Contact in writing the Director of Information Technology with a request for international service
- The request must allow enough time for *plus 24 hours for the wireless carrier to initiate service prior to international usage.* The request must include the dates the service is required, and the countries in which the service will be used
- A failure to initiate international service before usage will result in unauthorized charges under this policy. As such, these charges will become the employee's personal financial responsibility

Policy on Personal Usage and Personal Apps

The policy allows for reasonable personal usage of Webb Owned devices. Personal usage of a managed Service that results in a fee (e.g., download of apps, minutes/data overages) is the responsibility of the employee and must be reimbursed to Webb Institute in the month following billing. There is no expectation that employees reimburse Webb Institute for personal usage of Webb-owned devices of managed service if charges remain less than or equal to the standard monthly fee.
The policy prohibits employees from purchasing "apps", music, or other content for personal use with a Webb Institute account. If this activity occurs, the employee must provide evidence of reimbursement of these costs. When purchasing "apps" for personal use, employees must use their personal iTunes, Google Play, etc. accounts.

New York State Information Security Breach and Notification Act

- The "Information Security Breach and Notification Act," effective December 7, 2005, provides New York State residents with the right to know when a security breach has resulted in the exposure of their private information.
- The security breach covered by this law pertains to the unauthorized acquisition of computerized data which compromises the security, confidentiality, or integrity of private information.
- Private information, covered by this law, means any personal information in combination with any one or more of the following data elements: social security number, driver's license number, account number, or credit or debit card number in combination with any required security code.

This policy is maintained by the Department of Information Technology and shall not be revised without the written approval of the President of Webb Institute.

Faculty and staff should also refer to the "Webb Institute Employee Handbook" for further information on Webb's policies and procedures. Faculty should also refer to the "Faculty Handbook" for faculty-specific policies and students should refer to the Student Organization Handbook.

Webb Institute's Information Technology Policy: Acceptable Use of Artificial Intelligence (AI) and Network Security Guidelines

Applies To: All Students, Faculty, Staff, Researchers, Administrators, and Campus Guests

1. Purpose & Scope
This policy establishes secure operational boundaries for deploying and utilizing Local and Cloud-Based Artificial Intelligence (AI) technologies across campus networks and endpoint systems. It supports academic innovation while protecting campus infrastructure, network integrity, and confidential data (including FERPA and PHI compliance).

2. Core Security & Data Privacy Rules

- **Official Campus AI Catalog:** Webb Institute officially provides and supports **Google Gemini** and **Google NotebookLM** via institutional Workspace accounts. For all other AI tools, IT maintains an approved list of vetted AI tools, however technical support of those tools is not provided by Webb Institute's IT department.
- **AI Tool Risk Assessment:** All AI software, platforms, or browser extensions used for official college business must undergo an IT security risk and encryption assessment prior to adoption. Any request for AI tool approval must be sent to IT@webb.edu.
- **No Acceptable Use Exception (FERPA/PHI):** Entering Protected Health Information (PHI) or student records protected under the Family Educational Rights and Privacy Act (FERPA) into AI models is prohibited unless a specific, legally binding data-privacy agreement with the AI tool provider is obtained. By existing institutional accounts, internal data is considered protected when using Google Gemini tools.
- **Model Training Exclusions:** Official college operations must only utilize enterprise-tier AI licenses that explicitly guarantee user prompts and uploaded data are not saved or used to train future public models. Availability of additional AI tool licenses is provided at the discretion of individual departments, after initial safety approval from IT.

3. Local AI Models & Endpoint Infrastructure Security
Running local AI tools (e.g., Ollama, LocalAI, vLLM, LM Studio) introduces system-level vulnerabilities and network risks. The following restrictions apply across all endpoint hardware:

- **Environment Sandboxing:** Local AI models running on personal or college-owned devices must execute strictly inside an isolated virtual machine or container environment to prevent unauthorized system and hard drive access. Refer to instructions in Q:\StudentApps\AiVirtualization for instructions to do so.

- **Privilege Limitation:** Local AI agents, web interfaces, and developer scripts should be carefully reviewed before running with root or administrator privileges.
- **Network Isolation Boundaries:**
    - **Prohibited Networks:** Local AI hosts or API servers are strictly banned from connecting to the primary Wired LAN, official Faculty/Staff Wireless, and official Student Wireless networks.
    - **Guest Wireless Permission:** Devices running sandboxed local AI models may connect to the Guest Wireless Network, utilizing its built-in client isolation. Access to the Guest Wireless Network for Webb-issued devices can be obtained by request to the IT Department.
    - **AI Workstations:** Dedicated AI-enabled workstations managed by Webb may connect to the Wired LAN by a dedicated VLAN only.
- **Software Verification:** All open-source model weights, LLM binaries, and software packages must be verified against official software signatures prior to download.

4. Department Data Governance

- **Department Policy:** Each department at Webb Institute shall maintain department-level decisions on acceptable AI tool and data use. Refer to each department for specific policies.

5. Network Protections & System Defenses

- **Traffic Inspection & Threat Audits:** IT conducts continuous monitoring for rogue listening ports, shadow IT applications, unauthorized browser extensions, and high-frequency internal scanning behaviors that indicate un-sandboxed AI agents. Devices and users found in violation of the IT policy will be held responsible.
- **Bandwidth Controls:** IT reserves the right to throttle or terminate connections engaging in high-bandwidth model weight downloading, continuous training loops, or aggressive web scraping in the interest in maintaining service quality for all network users. Users may request a review of a network usage restriction by emailing IT@webb.edu.

Information Technology Policy: Workstation Gaming and Network Usage

1. Purpose

This policy defines the acceptable use of institutional workstations regarding video games and gaming software. The objective is to protect the institution's network infrastructure, data, and endpoints from malware, unauthorized software exploits, and cybersecurity vulnerabilities.

2. Scope
This policy applies to all students, faculty, staff, and authorized users operating institution-issued workstations, regardless of physical location or network connection (including the institutional network, Guest network, or home networks).

3. Workstation Gaming Restrictions
The institution utilizes advanced Endpoint Detection and Response (EDR) software, specifically SentinelOne, to monitor and secure all institutional devices.

- **Prohibited Software:** Any game or gaming platform blocked by the institution's Cyber AV software (SentinelOne) is strictly prohibited. If the gaming software triggers a block, users are not permitted to bypass, disable, or request an exception for the gaming software.
- **Security Rationale:** Gaming applications and platforms, particularly those utilizing Steam directories or similar distribution paths, are frequently targeted by malicious actors seeking to inject malware or exploit software vulnerabilities. Restricting these paths is necessary to safeguard the integrity of the endpoint.
- **Global Enforcement:** Endpoint protection is active directly on the workstation. Restrictions remain in effect whether the device is connected to the primary campus network, the Guest network, or an external home network.

4. Permitted Exceptions and Personal Devices
The institution recognizes that gaming can serve as a recreational outlet for students. To balance cybersecurity requirements with student recreation, the following exceptions are permitted:

- **Unblocked Games and Software on your Webb-issued computer:** Any gaming or recreational software on your Webb-issued workstation that is not currently restricted by endpoint security may remain unblocked. However, if SentinelOne blocks that software in the future, the restriction will stand with no exceptions.
- **Personal Devices:** Students and users are permitted to utilize privately owned personal computers, consoles, or mobile devices for gaming purposes.
- **Guest Network Access:** Personal devices should be connected to the institution's designated Guest network to access gaming services, provided such activity does not violate general network bandwidth or acceptable use policies. Institutional endpoint security policies do not apply to personal devices on the Guest network.

5. Compliance and Enforcement
Attempts to circumvent endpoint security controls, modify antivirus configurations, or install unauthorized software may result in a revocation of workstation privileges and referral to the appropriate disciplinary authority.