Acceptable Use Policy

POLICY TITLE: Acceptable Use Policy

POLICY CATEGORY: COLLEGE ADMINISTRATIVE

POLICY NUMBER:

POLICY VERSION: 1

POLICY OWNER: VP Digital Transformation and Chief Information Officer

APPROVAL DATE: Click or tap to enter a date.

EFFECTIVE DATE: Click or tap to enter a date.

POLICY APPROVER: Board of Governors

REVIEW PERIOD: Every 5 Years (or as needed)

REVIEWED: 6/24/2024

REVISED: N/A Click or tap to enter a date.

---

1. Purpose

This policy outlines the acceptable use of George Brown College's (“GBC”) Technology Assets and protects GBC Users. It defines and communicates specific practices permitted or prohibited when using GBC’s Technology Assets, including how GBC Information may be accessed, used, stored, processed, transmitted, and disposed of.

GBC is committed to providing all its Users with access to quality information systems and services to:

- Facilitate the delivery of the College's mandate offering a comprehensive program of career-oriented, post-secondary education;
- Assist faculty and staff in delivering high-quality and high-impact learning experiences;
- Support research and innovation opportunities; and
- Ensure the cost-effective, secure, and efficient management of the College's infrastructure.

2. Scope

GBC Technology Assets must primarily be used for working, academic learning, teaching, research, or support purposes.

This policy applies to all GBC:

- All users of GBC Technology Assets, including, but not limited to, students, employees, faculty, consultants, contractors, subcontractors, vendors, temporary workers, guests, trusted partners, alums, and agents of the GBC (collectively referred to as Users).
- GBC Technology Assets include but are not limited to GBC data, emails, Instant Messaging (IM), learning management systems, social media, networks, desktops, laptops, mobile devices, servers, storage media, cloud, on-premises, and physical documents.
- Users working either on or off GBC campuses, including any remote locations.

Additional questions on acceptable use should be directed to Information Technology Services.

3. Definition of Terms

Please see this link for all definitions.

4. Policy

4.1 General

4.1.1 This policy does not address every possible scenario; Users shall operate in a safe and respectful manner consistent with the expectations set out in this policy, using reasonable judgment.

4.1.2 The absence of a statement prohibiting a certain activity does not give tacit approval to conduct that activity.

4.1.3 Use of any GBC Technology Assets implies that the User has read the "Acceptable Use Policy" as it may be updated occasionally and unconditionally agrees to always abide by all terms and conditions.

4.1.4 GBC Technology Assets shall be used only for academic, learning, teaching, research, working, or support purposes.

4.1.5 GBC Technology Assets shall not be used for activities considered illegal, fraudulent, malicious, or otherwise violate any GBC policy or applicable standard or procedure. This includes accessing, sharing, viewing, downloading, storing, displaying, or distributing (sending or forwarding) images, text, or other content that is or could be considered indecent, discriminatory, offensive, or could affect GBC or other Users negatively.

4.1.6 GBC reserves the right to remove any data and material it deems inappropriate from its Information Systems and networks.

4.2 Personal Use and Electronic Monitoring

4.2.1 Limited personal use of GBC systems and IT services is permitted, provided that such use does not:

- Violate this policy or any other GBC policies.
- Interfere with work duties/performance.
- Negatively impact network or system performance.
- Limit the accessibility of shared college technology.
- Misrepresent GBC or negatively impact its reputation.
- Incur additional charges to GBC.
- Induce or substantially elevate the likelihood of a breach involving personal information.

GBC Technology Assets are not a substitute for personal technology. Users should not have an expectation of privacy consistent with transmitting or storing sensitive personal information using these Technology Assets.

4.2.2. GBC is committed to the security and privacy of its Technology Assets. Authorized GBC employees routinely review data within GBC Technology Assets to maintain system operations and security. While GBC does not routinely conduct active and manual reviews of emails, chats, documents, or similar items created or stored by Users, the authorized employees from the Information Technology Services (ITS) department may perform these reviews as part of ongoing responsibilities to protect the college and its community members.

4.2.3 Communication systems such as email are not secure by nature. While GBC takes reasonable precautions to secure its Technology Assets and systems, Users should exercise caution when using GBC technology for personal use.

4.2.4 It is the User's responsibility to remove or delete any personal data/information copied to or saved on GBC equipment/systems before the User's departure or graduation from the College. Personal files not deleted or removed, including those identified explicitly as Personal, will be retained and/or deleted as required by GBC policy and applicable laws.

4.2.5 All resources, files, records, or other information created, processed, or stored using GBC Technology Assets may be accessed by authorized GBC employees at any time.

4.2.6 GBC Technology Assets are monitored for various legitimate purposes, including system analysis, operational planning, system performance, determining unacceptable resource use, complying with legal obligations, and supporting GBC investigations. ITS employees monitor activities per applicable laws, regulations, and procedures established by GBC's Cyber Security team, legal counsel, and/or Chief Information Officer. Nothing in this policy should be construed to mean that authorized GBC employees actively view personal information without an approved purpose.

4.2.7 GBC may also be obligated to disclose email and Instant Messaging (IM) messages and conversations when ordered by auditors, courts, and law enforcement, with or without the User's consent.

4.3 Expectations and Responsibilities for All Users

4.3.1 Users are responsible for using GBC Technology Assets per all GBC policies, including this policy.

4.3.2 Each User is accountable for using any GBC Technology Asset and any actions carried out using their GBC account.

4.3.3 Users are responsible for protecting their GBC login credentials and securing GBC Technology Assets against unauthorized use or access. Users shall not share their login credentials.

4.3.4 Users shall store files and documents on GBC-approved network/cloud systems, such as GBC-provided OneDrive, SharePoint, or other GBC-provided systems, and not on local computers and laptops' hard drives (C:). In exceptional cases where this policy statement cannot be followed, the files and documents shall be copied to the network/cloud as soon as possible.

4.3.5 Users shall not attempt to disable, defeat, circumvent, or otherwise tamper with any installed GBC security measures or attempt to use or install unauthorized software or hardware.

4.5.6 All Users are responsible for monitoring their georgebrown.ca email account for notices and correspondences from the College.

4.5.7 All Users should maintain a Cyber Security vigilant mindset, stay updated on new threats highlighted by the college, follow Cyber Security guidelines, and use appropriate tools the college provides to protect GBC Technology Assets. Users shall immediately notify GBC Cyber Security should they discover any suspected or actual unauthorized access to or use of GBC Technology Assets.

4.6 Prohibited Activities for all Users

Users shall not use GBC Technology Assets to:

4.6.1 Violate any law or encourage others to violate any law.

4.6.2 Engage in discrimination or harassment based on a Prohibited Ground.

4.6.3 Violate any other GBC policy or Code of Conduct.

4.6.4 Conduct fraudulent activity.

4.6.5 Monitor, eavesdrop, scan, intercept, interrupt, alter, and/or compromise the GBC network, systems, or resources unless authorized to do so by GBC Cyber Security.

4.6.6 Intrude into the networks, systems, data files, or devices of others.

4.6.7 Eavesdrop or monitor the activities of others unless authorized.

4.6.8 Use, access, or disclose others' information without authorization.

4.6.9 Download, install, use, or distribute software for which they do not have a license and authorization.

4.6.10 Create or distribute malware or other disruptive/destructive constructs.

4.6.11 Use another person's credentials (username or password) for any reason.

4.6.12 Impersonate another person.

4.6.13 Unnecessarily or unreasonably waste bandwidth, server time, storage space, or other resources.

4.6.14 Operate a for-profit/commercial or non-profit business without authorization.

4.6.15 Distribute bulk mail (spam), chainmail, or other messages for unauthorized purposes.

4.7 Additional Expectations and Responsibilities for All Employees

4.7.1 Personal emails shall not be used to conduct GBC work/business (e.g., Sending and receiving work emails, documents, and files through Gmail/Hotmail/Yahoo). This includes forwarding GBC emails to any personal email accounts unless explicitly approved by Cyber Security. However, documents pertaining exclusively to the employee's own employment, such as pay or employment-related communications from HR or the employee's union, may be forwarded to a personal email account. GBC email (georgebrown.ca) is the only approved email solution for communication, correspondence, notifications, and delivery of information via email.

4.7.2 Email is an insecure method of communication. Sensitive or personal information shall not be sent via email attachments or in the body of the email without approval from the information owner or responsible manager, regardless of the recipient or urgency.

4.7.3 When sharing (sending or receiving) sensitive files externally, OneDrive, SharePoint, or other secure GBC systems shall be utilized instead of email attachments.

4.7.4 Users shall not host or post information on blogs, chat rooms, user groups, discussion forums, social networking sites (e.g., Facebook, Twitter, LinkedIn, Instagram, Reddit), or other forms of Internet-based communications that could jeopardize the

security or privacy of GBC or others, violate GBC policies or codes of conduct, or break any applicable laws.

4.7.5 GBC Social Media Assets shall not be used for non-work-related activities.

4.7.6 All GBC technology Assets (including GBC information/data) shall be returned to GBC upon termination of employment or contract or during an extended leave of absence.

4.7.7 Managers and leaders are responsible for ensuring their employees understand and adhere to this policy's stipulations.

4.7.8 Faculty members are responsible for ensuring that students are aware of this policy and redirect any questions about it or its provisions to the Cyber Security team.

4.7.10 Contract owners are responsible for ensuring that any third parties (vendors, contractors, etc.) providing services and solutions to the college understand and adhere to this policy's stipulations.

5. Compliance and Enforcement

5.1 This policy serves as the guiding document for all GBC Users. Users are expected to adhere to this policy and seek clarification on ambiguous aspects.

5.2 Any non-compliance or policy violation should be reported to Cyber Security, the Vice President, Digital Transformation & Chief Information Officer, or the Vice President, People and Culture.

5.3 GBC reserves the right to reasonably investigate any actual or suspected breaches of this policy.

5.4 Employees who violate the "Acceptable Use Policy" may be subject to disciplinary action up to and including employment termination in alignment with applicable collective agreements.

5.5 Students/learners who violate the "Acceptable Use Policy" may be subject to disciplinary action, up to and including expulsion, per the applicable codes of conduct and academic policies.

5.6 Vendors, contractors, sub-contractors, temporary workers, guests, trusted partners, and guests who violate the "Acceptable Use Policy" may have their contracts terminated, accounts suspended, and/or be refused access to GBC campuses and services.

5.7 GBC reserves the right, at its discretion, to permanently revoke access to any GBC Technology Assets and services at any time.

5.8 Users who violate Municipal, Provincial, Federal, or international law may be subject to criminal prosecution and/or civil litigation by the appropriate authorities.

6. Exceptions

While adherence to this policy is mandatory for all GBC Users, the VP, Digital Transformation & CIO may grant an exception under exceptional circumstances where compliance may not be feasible or could impede legitimate operational requirements. The approval shall be time-bound and not regarded as an indefinite waiver.

Related Materials

This policy is aligned with the ISO 27000 family of standards (Information Security Management System (ISMS)).

ISO Standards:

- ISO 27001: Information Technology – Security Techniques – Cybersecurity Management System (ISMS) - Requirements

Related Policies

Employee Code of Conduct - Staff	**Cyber Security Policy**	**Employee Code of Conduct – Academic**	**Employee Code of Conduct - Admin**
Privacy Policy	**Code of Non-Academic Student Behaviour**		