POLICY:

Georgia Perimeter College requires users to use Information Technology resources in a responsible manner.

PROCEDURE:

Privileges and procedures are provided below for applicable users and for GPC. Applicable users include all faculty, staff, retirees, students, contractors, subcontractors, and GPC guests.

User Privileges

Privacy

Electronic and other technological methods will not be used to infringe upon privacy. However, GPC computer systems and networks are public, the property of the State of Georgia, and as such, are subject to the Georgia Open Records Act. Users should utilize such systems with the awareness that college computing resources are not to be treated in the same manner as one’s personal computing resources.

Ownership of Intellectual Works

Users creating intellectual works using GPC computers or networks, including but not limited to software, should consult Determination of Rights and Equities in Intellectual Property (Board of Regents Policy Manual, Section 6.3.3 and any subsequent revisions), and any related GPC policies.

Freedom from Harassment and Display of Objectionable or Undesired Material

All members of the institution have the right not to be harassed by computer or network usage by others.
User Procedures

1. **Users should only use those computing and IT resources for which they have authorization. It is a violation for users to do the following:**
   - Use resources they have not been specifically authorized to use.
   - Use another person’s account and password or share their account password with someone else.
   - Access files, data, or processes without authorization.
   - Purposely look for or exploit security flaws to gain system or data access.

2. **Protect the access and integrity of computing and IT resources. It is a violation to do the following:**
   - Use excessive bandwidth.
   - Release a virus, worm, or other malicious software that damages or harms a system or network or accesses data.
   - Prevent others from accessing an authorized service.
   - Send email that may cause problems and disrupt service for other users.
   - Attempt to deliberately degrade performance or deny service.
   - Corrupt or misuse information.
   - Access, alter, or destroy information without authorization.

3. **Abide by applicable laws and GPC policies and respect the copyrights and intellectual property rights of others, including the legal use of copyrighted software. It is a violation to do the following:**
   - Use peer-to-peer software or other means to unlawfully download, use, or distribute copyrighted materials, including pirated music, videos, software, or games.
   - Make more copies of licensed software than the license allows.
   - Upload, download, distribute, or possess pornography.
   - Upload, download, distribute, or possess child pornography.

4. **Use computing and IT resources only for the intended purposes. It is a violation to do the following:**
   - Use computing or network resources for advertising or other commercial purposes.
   - Distribute copyrighted materials without express permission of the copyright holder.
   - Send forged email.
   - Misuse Internet Relay Chat (IRC) software to allow users to hide their identity or to interfere with other systems or users.
   - Send terrorist threats or "hoax messages."
   - Send chain letters.
   - Intercept or monitor any network communications not intended for the user.
   - Attempt to circumvent security mechanisms.
   - Attempt to introduce any unauthorized software or technologies (e.g., unapproved third party software, malicious software) into the GPC processing environment.
• Use privileged access for other than official duties.
• Use former privileges after graduation, transfer, or termination, except as stipulated by GPC.

5. **Respect the privacy and personal rights of others. It is a violation to do the following:**
   • Use electronic resources for harassing or stalking other individuals.
   • Tap a phone line or run a network sniffer or vulnerability scanner without authorization.
   • Access or attempt to access other individual's password or data without explicit authorization.
   • Access or copy another user's electronic mail, data, programs, or other files without permission.
   • Disclose information about students in violation of GPC policies and applicable laws (e.g., FERPA).

6. **Use of computer systems**
   Users are responsible for the security and integrity of college information stored on their assigned college system. Users must control physical and network access to the machine, make regular backups, and use available virus protection. GPC reserves the right to electronically inspect a user's computer for the appropriate levels of antivirus, spyware, operating system, and other security measures before allowing access to GPC network computing resources.

   Off campus use of equipment is permitted with appropriate approvals. The reporting department will be financially responsible for the insurance deductible of up to $1000.00 for the replacement of equipment resulting in loss due to negligence, inappropriate use, theft and/or repairs due to non-warranty damage. Departments will be responsible for determining whether individual staff will be held financially accountable for any portion of said deductible.

7. **Political campaigning and commercial advertising**
   Board of Regents policy (section 9.10.6.1) states “The use of USG materials, supplies, equipment, machinery, or vehicles in political campaigns is forbidden.” The use of college computers and networks shall conform to these policies.

8. **Personal business**
   Computer facilities, services, and networks may not be used in connection with outside work or for the benefit of organizations not related to GPC except in connection with traditional scholarly pursuit. State law restricts the use of state facilities for personal gain or benefit.

**Georgia Perimeter College Privileges**

GPC has been granted by the State and various other organizations certain privileges regarding the information resources necessary to accomplish the mission of the college.

**Control of access to information**

Georgia Perimeter College may control access to its information and the devices on which it is stored and transmitted, in accordance with the laws of Georgia, the United States, and the
policies of the college and the Board of Regents.

**Imposition of sanctions**
Georgia Perimeter College may impose sanctions on anyone who violates the policies of the college regarding computer and network usage.

**System administration access**
System administrators and providers have the responsibility of ensuring the confidentiality, integrity, and availability of IT resources. The persons in these positions are granted significant trust to use their privileges appropriately, and these privileges must be used only for assigned job responsibilities. Individual privileges and rights of privacy are to be preserved to the greatest extent possible, unless a violation of policy or compromise of security occurs.

**Monitoring of usage and inspection of files**
Georgia Perimeter College may routinely monitor and log usage data, such as network session connection times and end-points, CPU and disk utilization, security audit trails, and network loading. Data may be reviewed for evidence of violation of law or policy and other purposes.

**Suspension of individual privileges**
GPC information resource privileges may be suspended for reasons relating to the safety and well-being of members of the campus community or college property. Access will be promptly restored when safety and well-being can be reasonably assured, unless access is to remain suspended as a result of formal disciplinary action imposed by the institution.

**Georgia Perimeter College Procedures**

1. **Security procedures**
   Georgia Perimeter College will develop, implement, maintain, and enforce appropriate security procedures to ensure the confidentiality, integrity, and availability of individual and institutional information and will impose appropriate penalties when security is purposefully abridged.

2. **Anti-harassment procedures**
   Georgia Perimeter College will develop, implement, maintain, and enforce appropriate procedures to discourage harassment by use of its computers or networks and will impose appropriate penalties when such harassment takes place.

3. **Upholding of copyrights and license provisions**
   Georgia Perimeter College will uphold all copyrights, laws governing access and use of information, and third party contract and license provisions.

4. **Individual department procedures**
   Each department will ensure that personnel within the department understand and comply with this policy and associated procedures, protect the confidentiality of sensitive or personal data, and comply with applicable information security policies and procedures. The Office of Information Technology serves as the first point of contact for college personnel seeking
problem resolution, information, and other assistance regarding information resources.

5. **Public information services**
Departments and individuals may not configure college computing systems to provide information retrieval services to the public at large.

**General Procedures**

1. **Investigative contact**
Any member of the college community contacted by a representative from an external organization (District Attorney’s office, FBI, GBI, etc.) conducting an investigation for an alleged violation involving Georgia Perimeter College computing and networking resources should immediately inform the Office of Information Technology and the Office of Human Resources. Refer the requesting agency to the OIT office. OIT will provide guidance regarding the appropriate actions to be taken.

2. **Responding to security and abuse incidents**
   All users and units have the responsibility to report any unauthorized access attempts or other improper usage of GPC computers, networks, or other informational processing equipment. If users observe or receive information regarding a security or abuse problem with any GPC information resource, including violations of this policy, they should:
   - Ensure personal and personnel safety;
   - Immediately contact the OIT Service Desk with a description of the issue.

   OIT will provide the technical and administrative response to such incidents.

3. **Sanctions**
   Persons in violation of this policy are subject to a range of sanctions (determined and enforced by GPC management), including the loss of computer network access privileges, disciplinary action, dismissal from the college, and legal action. Some violations may constitute criminal offenses, as outlined in the Georgia Computer Systems Protection Act and other local, state, and federal laws. The college will carry out its responsibility to report such violations to the appropriate authorities. Appeals should be directed through the existing procedures established for employees or students.