Policy Number: 506

Policy Title: Third Party Software

AAPC: Many of the faculty members on the AAPC expressed concern with this policy. The Council also received comments from other faculty members who were concerned that this policy is too restrictive. Some felt that FERPA was being used to justify restrictions that aren’t a part of the law’s requirements. The policy seems to make no differentiation between social media and sites designed for strictly educational purposes. The approval process isn’t specified and rests the authority to approve or disapprove in one person, the Chief Information Security Officer. Faculty were unsure whether this policy extends to publisher software that resides outside of the iCollege portal but which is part of an approved textbook adoption. Many of our current practices seem to violate this policy. Faculty believe that educational benefit must also be a part of the consideration.

POLICY:

Faculty and staff will only use software applications and services provided by the Georgia Perimeter College to conduct official business with students and each other. These College-provided applications and services ensure that: 1) appropriate information security procedures are used, 2) individual privacy rights are protected, and 3) Georgia Perimeter College intellectual property rights are preserved. Use of any third-party application software or service not provided by the College requires approval of the Office of the Chief Information Officer and the Chief Information Security Officer, who will ensure that appropriate contractual safeguards are in place.

PROCEDURE: [This is policy, not procedure.]

The current trends in either “cloud-based” services and personal social networking applications (Facebook, mySpace, Twitter, etc.) have caused many faculty and staff to consider using these popular products or services as adjunct communication tools for either performing routine business activities, or conducting teaching and learning. This is problematic because of several reasons:

1) If any information provided in these applications is related to a student’s enrollment in courses or academic activities at the College, this could be a Family Educational Rights and Privacy Act (FERPA) violation.
2) These applications may not provide adequate confidentiality or privacy for participants, and can result in exposure of sensitive or personal information.
3) Intellectual property rights of whatever is posted to these sites or through these services are usually relinquished by the user of the site to the application provider.

4) Individuals participating on these sites do not require certifiable identification and authentication, i.e., it is too easy to “spoof” other people, and could result in unauthorized access or modification of the information.

5) The College is exposed to risks like reputational loss, etc., and does not have control over the content that has been posted or transmitted via the third-party product.

This policy applies to all GPC faculty and staff. The Chief Information Officer and Chief Information Security Officer are responsible for assessing and approving requests for any software or services not provided by the College.

To appropriately protect GPC’s valuable and sensitive information, including personal information of the students, faculty, and staff, all applicable users are required to comply with this policy. Persons in violation of this policy are subject to a range of sanctions, 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.

The Chief Information Officer will establish procedures to review requests for approval of use of third-party products. These procedures will address responsibilities of the CIO and the CISO to attempt to facilitate use of the products, yet protect the College’s rights and interests, and adequately safeguard any related data. If possible, the CIO may engage Legal Affairs to secure contractual relationships that would still enable use of the desired services, but not expose the College to risk.

“Official business” includes interaction between students, faculty or staff as it relates to: delivery of course content or materials, information exchange that is related to a student’s academic performance, required learning activities, taking of for-credit courses, fiscal or financial transactions, or involves transmittal of personally identifiable or other sensitive data that is protected information under legal or regulatory requirements (e.g., FERPA, Health Insurance Portability and Accountability Act, identity theft laws).

PPAB Approval Date: ________________________________

Policy Council Review Date(s):
ITPC: 1/27/12