

Central Penn College Information Technology (I.T.) Policy

Approved by Technology Steering Committee, July 20, 2011

The vision of Central Penn College includes a call to embrace “today’s technology.” This policy exists to further that vision and ensure all members of the Central Penn community have the information technology tools, training, and support they need to be successful.

Section 1: The Technology Partnership

The successful implementation and use of information technology requires a partnership and ongoing dialogue between students, faculty, staff, and the I.T. Department. In addition to I.T. topics, all stakeholder groups must communicate major non-I.T. initiatives to the I.T. department so it can adjust policies, procedures, personnel, system capacity, and configuration accordingly.

1.1 Students

I.T. needs, challenges, and ideas, affecting a large number of students should be communicated through the Student Government Association. The I.T. Director will attend Student Government Association meetings upon request. Individual problems and questions should be submitted to the appropriate help desk as published.

1.2 Faculty

High-impact faculty needs, challenges, and ideas should be communicated through the Faculty Senate or Academic Council. The I.T. Director will attend Faculty Senate and Academic Council meetings upon request. Low-impact faculty needs should be communicated directly through meetings with the I.T. Department. Individual problems and questions should be submitted to the appropriate help desk as published or discussed with the I.T. Education Specialist. The Faculty Senate should keep the I.T. Department apprised of discussions about possible future changes so the department can support those initiatives.

1.3 Staff

High-impact staff needs, challenges, and ideas should be communicated through the Strategic Goal Facilitators (S.G.F.s) or Senior Leaders. The I.T. Director will attend S.G.F. and Senior Leader meetings upon request. Low-impact staff needs should be communicated directly through meetings with the I.T. Department. Individual problems and questions should be submitted to the appropriate help desk as published. The S.G.F.s and Senior Leaders should keep the I.T. Department apprised of discussions about possible future changes so the department can support those initiatives.

1.4 I.T. Department

The I.T. Department mission is “stay current with technology trends and make utilization of technology easier for students, faculty, and staff through advising, teaching, automating, and troubleshooting.” To support that mission, the department shall regularly gather input from stakeholders to develop plans,

budgets, policies, procedures, and training. It shall communicate relevant information to the Central Penn community through a variety of media.

1.5 Technology Steering Committee

At least quarterly, the I.T. Director shall convene a task force representing the above groups to approve strategies, policies, and projects. The group shall include, at a minimum, a Senior Leader, a professor, an academic administrator, a non-academic administrator, a residential student, a non-residential student, and a graduate.

Section 2: Excellence Through Standardization

To maintain a reliable infrastructure serving thousands of stakeholders across multiple campuses, buildings, rooms, and offices requires adherence to standards for hardware, software, networks, installation, configuration, projects, changes, and security.

2.1 Hardware and software standards

With input from stakeholders, the I.T. Department shall set standards for computers, servers, printers, networks, copiers, and similar devices as well as for software to run on those devices. Standards must take into consideration the unique needs of each academic program.

2.2 Purchasing and installation standards

The I.T. Department shall purchase or otherwise acquire all hardware and software, and work with the Business Office for proper accounting of purchases and tracking of assets. To ensure compatibility, security, and reliability, all installations will be performed by I.T. Department personnel or its designated vendor.

2.3 Safety and security standards

To maintain safe, reliable infrastructure, the I.T. Department shall set standards related to device configuration, user access privileges, network usage, virtual security, storage, and physical security of I.T. resources.

2.4 Project management methodology

The I.T. Department shall maintain an effective methodology for managing projects. The department shall use that methodology to manage all I.T. projects. In cases where another party is assigned responsibility for an I.T. project, they may either delegate management of that project to the I.T. department, or manage it using the project methodology.

2.5 Reporting standards

The I.T. Department will produce accurate, useful reports for the organization, and provide tools and training so end users can create their own reports.

2.6 Moves, add, and change process

To ensure all hardware and software is configured to the required specifications, the I.T. Department or its designated vendor will receive, document, acquire approvals for, and administer all technology-related moves, adds, and changes.

2.7 Technical support

To maintain a consistent level of support, the I.T. Department will publish support procedures for all systems that may involve in-house and outsourced components. Both internal and external support providers will document and track all requests received through the proper channels.

Section 3: Community Rights and Responsibilities

3.1 Everyone has a right to reliable systems and support.

3.2 Everyone is responsible for respecting and protecting the privacy of others, and must...

Use only assigned accounts;

Not view, use, or copy passwords, data, or networks to which they are not authorized;

Not distribute passwords or similar private information about others or themselves.

3.3 Everyone is responsible for respecting and protecting the integrity, availability, and security of resources, and must...

Observe all network security practices;

Report security risks violations;

Not destroy or damage data, networks, or other resources that do not belong to them;

Conserve, protect, and share I.T. resources with others;

Report any problems discovered as soon as possible.

Faculty teaching information security and related topics may interpret this section as needed to allow the necessary learning to take place without negatively impacting other areas of the college.

3.4 Everyone is responsible for respecting and protecting the intellectual property of others, and must...

Not infringe copyrights (i.e. the making of illegal copies of music, games, or movies);

Not plagiarize.

3.5 Everyone is responsible for respecting and practicing the principles of community, and must...

Communicate only in ways that are kind and respectful;

Report threatening or discomforting materials;

Not intentionally access, transmit, copy, or create material that violates school policies (such as messages that are pornographic, threatening, rude, discriminatory, or meant to harass);

Not intentionally access, transmit, copy, or create material that is illegal (such as obscenity, stolen materials, or illegal copies of copyrighted works);

Not use the resources to further other acts that are criminal or violate the school's code of conduct;

Not send spam, chain letters, or other mass unsolicited mailings;

Not buy, sell, advertise, or otherwise conduct business, unless approved as a school project.

3.6 The I.T. Department and vendors have the right to advanced notice for move, add, and change requests.

3.7 Management has the right to view emails and other normally-private documents stored on school systems. They shall exercise this right infrequently and judiciously.

3.8 Violations of any section of the I.T. policy may result in disciplinary action for students, faculty, and staff.