

Stautzenberger College Internet, E-mail, and Technological Resources Guidelines

Stautzenberger College prides itself on the technological resources it offers its students, staff and faculty. Because the College offers internet access both on its own computers and wirelessly, members of the college community enjoy enormous flexibility and access to broad internet resources. With such access, however, comes responsibility as well.

Every member of the Stautzenberger College community who chooses to use either the hardwired or wireless internet resources is subject to the following rules:

1. All users must observe Stautzenberger College standards concerning security, ethics, conduct, and protocol, including ensuring that all uses are conducted with consideration and respect for both College property and members of the College community;
2. All users must respect the privacy of other users,
3. All users must respect civil, criminal, copyright, trademark and patent law in the use of College internet resources and equipment, and
4. All users must respect the integrity of the College's computing systems.

If a member of the Stautzenberger College community chooses to engage in an unacceptable use of the internet, computer network or other technological resources of the College, he or she will be subject to immediate discipline.

Unacceptable use includes, but is not limited to:

1. Illegal or inappropriate use of college facilities,
2. Activities that may interfere with or disrupt network users, services or equipment; or
3. Displaying sexually explicit, graphically disturbing, or sexually harassing images or text on a college computer.

The following activities are expressly forbidden and will result in immediate dismissal or termination:

1. Using computer programs or other means to decode or attempt to decode passwords or access or attempt to access controlled or confidential information;
2. Attempting to circumvent or subvert system or network security measures, including creating and/or running programs that are designed to identify security loopholes and/or decrypt intentionally secure data;
3. Connecting or attempting to connect unauthorized equipment to the campus network, including any hubs and switches;
4. Engaging in any activity that might be purposefully harmful to systems or to any information stored thereon, including creating or propagating viruses or worms; disrupting services; damaging files; or making unauthorized modifications to College data;
5. Making or using illegal copies of copyrighted materials or software, storing such copies on College systems, or transmitting them over the college network;

6. Using e-mail or messaging services to harass, offend, or intimidate another person, whether by use of the College network or otherwise. This includes broadcasting or posting unsolicited messages, sending unwanted e-mail, or using another's name or user ID;
7. Impairing computing or network resources by intentionally placing a program in an endless loop, or by sending chain letters or unsolicited mass mailings;
8. Transmitting, downloading, retrieving, or storing any materials that are obscene, pornographic or X- rated;
9. Transmitting abusive, profane or offensive language using the college's e-mail or Internet system. Use of the college Internet system for gambling is also prohibited;
10. Transmitting e-mail messages or posting comments to social networks or blogs that include derogatory or inflammatory remarks about an individual's race, age, disability, religion, national origin or, physical attributes;
11. Harassing behavior of any kind is prohibited; and
12. Engaging in any other activity that does not comply with the Standards of Conduct.
Electronic media may not be used for a purpose that is against any other College policy.

Any activity that creates, downloads, or otherwise causes sexually explicit pictures or language to appear on computers under the control of an individual will be treated as an example of creating an intimidating, offensive, or hostile working/educational environment, and is a violation of these guidelines.

Consequences of Failure to Comply:

Stautzenberger College policies dictate that all members of the College community act in accordance with these responsibilities, applicable laws, relevant contractual obligations, and the highest ethical standards. The College considers any violation of these guidelines a serious offense. As a means of ensuring compliance with these policies, the College reserves the right to copy and examine any files or information stored on College systems potentially related to unacceptable use and to protect its network from systems, actions and events that threaten to or degrade operations. All users of the College's computing facilities are responsible for understanding the guidelines articulated above. Failure to comply with these guidelines may result in suspension of technology privileges at the College, or in civil or criminal action pursuant to state or federal law. Violators will be referred for disciplinary action, up to and potentially including dismissal or termination. The College further reserves the right to notify appropriate officials of potential violations of any law.

Monitoring:

All e-mail messages and comments created, sent, or retrieved over the College's e-mail, networks or internet systems are the property of Stautzenberger College, and should be considered public information. The College reserves the right to access and monitor all messages and files on the College's e-mail, networks and internet systems. Members of the College community should not assume electronic communications are private, even if such communications are protected by encryption. If the users wishes to ensure confidentiality of such communications, the user should transmit confidential data by non-College means.

Agreement:

I understand that it is my responsibility to abide by this Internet Use Policy, and that I am responsible for any use under my user account. I understand that the College may monitor my computer and Internet activity. I expressly consent to such monitoring. I further understand that failure to follow these guidelines shall result in appropriate discipline by the College and/or legal action.

I further understand that my right to access the College resources (including e-mail) ceases upon my graduation, withdrawal, termination or dismissal from the College. When access ceases, I understand that my login and e-mail account will be removed and all files associated with my account will be deleted.

This policy has incorporated elements of the policies of the following institutions: Baker College; Ozark Christian College and Skyline College.