Wabash.

Electronic Media, Services, and Communication Policy for Students

September 2, 2020

Introduction

Wabash College's ("Wabash" of "the College") technical resources, including any hardware, software, voicemail, email, Internet access, smart phones, copiers, scanners, facsimile machines, or other electronic resources provided by the College (College Resources) are intended to be used in the pursuit of official Wabash business. This policy expresses Wabash's philosophy and sets forth general principles to be applied to the use of College Resources even as technology evolves. College Resources also include, but are not necessarily limited to, all data and messages created, sent, received, or stored in the system; Internet facilities; facilities and services of the web site; domain names; social media handles, and email account names.

General Principles

The Wabash community values civility, honesty, fact-based conversation, and humane concern for others. At the same time, the College recognizes that electronic communications, including social media, have the potential to carry this discourse far beyond the walls of this institution. Because electronic communications such as email are not face-to-face modes of communication, users may be less cautious or more candid in the content of messages. Wabash requires that users of College Resources exercise due caution in the use of College Resources and social media.

The use of College Resources is subject not only to this Policy, but also to all other applicable College Policies, as well as local, state, and federal laws, rules, and regulations. College Resources should not be used to send jokes, comments, or messages that contain content that may be reasonably considered discriminatory, harassing, or defamatory. Email or other electronic communications, which attempt to hide the identity of the sender or creator, or represent the sender or creator, or misrepresent the sender as someone else, are violations of this Policy and the law.

Electronic media and services are primarily for educational use. Use of electronic media (sending or

Confidentiality and Security
Although electronic systems may accommodate the use of passwords for security, confidentiality cannot be guaranteed. Even though a file or email may be deleted from the system, a record of it may remain on the computer system either in backups or archived files or in other ways. It is possible to recreate a "deleted" file or email message. Therefore, ultimate privacy of messages cannot be ensured.

Messages and other information on these systems may be subject to the investigation, search, retrieval, and review by others in accordance with this Policy or when the investigation serves the legitimate business interests and obligations of Wabash. For purposes of inspecting, investigating, or searching Wabash's computerized files, transmissions, voicemail, or email, Wabash may override any applicable password or codes in accordance with the best interests of the College, its employees, or its students, prospective students, alumni, or visitors. All log files and other documentation related to the use of Wabash equipment or property may be reviewed and used for purposes that Wabash considers appropriate.

Email
The College's email system is not a private communication system (even though passwords are used for security reasons), and students should not expect that a message would never be disclosed to or read by others beyond its original intended recipients. Students should keep in mind that when they are using email, they are creating Wabash documents using an organizational asset. Students have no right of privacy to any information or file maintained in or on Wabash property or by using College Resources.

Students should be aware that electronic messages and documents, like "hard copy" correspondence, and other data or information created or accessible through College Resources might be read by other persons at Wabash or outsiders under circumstances similar to those under which the College may need to access other business files and information. While it is impossible to list all of the circumstances, some examples are the following:

- During regular maintenance of the system.
- When Wabash receives a legal request to disclose email or other electronic information from law enforcement officials or in ongoing legal proceedings.
- When Wabash has reason to believe that a student is in violation of the law or College policies.

Websites and Social Media
Network services and World Wide Web sites can and do monitor access and usage and can identify at least which College – and often which specific individual – is accessing their services. Thus, accessing chat rooms, message boards, or virtually any website leaves institution-identifiable electronic "fingerprints," even if the student merely reviews or downloads the material and has not posted any message.

Social media has become ubiquitous in our lives. Students should use personal email accounts in connection with non-Wabash-related Internet postings, e-commerce, social media interactions, and the like.

It is imperative that users adhere to federal and College policies related to privacy, including the Family Educational Rights and Privacy Act ("FERPA"), NCAA regulations, and any other applicable laws or policies.

Wabash College and Its Social Media Presence

The Communications and Marketing Office manages content on official Wabash social media channels, including but not limited to, Facebook, Twitter, Instagram, Snapchat, YouTube, LinkedIn, and its Podcast platform. An official Wabash channel is any channel that is accessible from the Wabash website.

In conjunction with IT Services, the Communications and Marketing Office must grant approval for any Wabash social media channels or accounts that bear the Wabash name or contain official logos or marks. This ensures adherence to policy and design standards of the College. Account managers must use a Wabash College email address for the account. The Communications and Marketing Office has the right to shut down any Wabash-related accounts that become stagnant. Before starting or maintaining a social media presence for your club, living unit, or sports team, contact the Communications and Marketing Office. Staff can suggest appropriate frequency of posts, ensure brand and logo consistency, and provide recommendations for marketing the channel and monitoring its success.

What students post on Wabash-affiliated social media platforms is the user's responsibility. Students should keep in mind that any posts could reflect directly on the College and could be perceived as coming from the College. Accuracy of facts, proper spelling and grammar, and strict adherence to privacy policies are critical.

Personal Social Media Accounts

Please do not use official College logos on personal social media sites without permission. Respect the privacy rights of students, faculty, staff, and alumni, and abide by FERPA, NCAA regulations, and any other applicable laws or policies regarding privacy and confidentiality.

Generally, the College considers use of social media to be a personal endeavor. Regardless, use of social media – even for purely personal purposes – presents certain risks and carries with it certain responsibilities. The student is ultimately responsible for what he posts online. A student should never represent himself or herself as a spokesperson for the College.

Student posts on social media that contain complaints or criticisms should not contain content that reasonably could be viewed as discriminatory, violent, vulgar, obscene, threatening, intimidating, harassing, slanderous, or similarly unlawful. Examples of such conduct might include offensive posts intended to intentionally harm someone's reputation or posts that could contribute to a hostile

educational environment based on race, sex, disability, religion, or any other status protected by law or College policy.

Ownership of Electronic Systems and Services, Confidentiality, and Copyright Issues
College Resources are and remain at all times the property of Wabash. Students should restrict access