Constituent Communications

VPCM-03

About This Policy

Effective Dates:
01-16-2019

Last Updated:
01-16-2019

Responsible University Administrator:
Vice President for Communications and Marketing

Policy Contact:
Rob Zinkan
Associate Vice President for Marketing
Office of the VP for Engagement

Greg Polit
Director, Informational & Emerging Technologies
Indiana University Communications
gpolit@iu.edu

Scope

This policy applies to all university units and to individuals, including all faculty and staff, engaging in constituent communications on behalf of any university unit or using university information technology resources. This policy is intended to govern communications that pertain to university engagement activities, and does not apply to individual academic communications among faculty and students or to operational communications.

Policy Statement

1. Only authorized individuals or units are expected to conduct engagement communications and/or official communications on behalf of Indiana University covered under this policy. Such communications should be for purposes of providing information, facilitating operations, or developing and maintaining relationships with the university's constituents. Communications should usually be broad-based approaches (e.g. direct mail, digital, phone, events); however, communications may be undertaken on an individual basis in some cases.
2. For purposes of communications, all constituents "belong" to the university as a whole, not to any individual unit or subset of the university. Engagement with constituents should be governed primarily by whether such engagement benefits the university as a whole and, secondarily, by whether it benefits any particular unit or program. While the university data stewards will act on behalf of the university to make institutional data available only to authorized individuals or units, those individuals and units are responsible for the messages they send.
3. Individual constituents and constituent groups are managed by university officials or offices for purposes of relationships and communications, and such assignments are governed by major constituent characteristics (e.g. student, faculty, campus, etc.). The constituent domains include:
    - Students (Prospects, Applicants, Admitted, Enrolled)
    - Faculty
    - Staff
    - Advancement (Alumni, Donors, and Prospects)

- Parents
- Political and government entities
- Research, contracts, and grants (including collaborators, research subjects and research sponsors)
- Patients
- Compliance agencies
- Other constituents with a relationship or potential relationship to IU

Constituent domains may have a Data Steward responsible for publishing standards and approval procedures for contacting members of their specific constituent group. In addition, university policies may apply to certain constituent contacts (i.e., GR-01).

4. Individuals and units given access to constituent information must ensure that the communication will not alienate the constituent, undermine other activities involving the constituent, or otherwise be detrimental to the interests of the university. Individuals and units must comply with any applicable state and federal laws governing the appropriate use and confidentiality of constituent information, including but not limited to constituent preferences, and, where applicable, FERPA, HIPAA, CAN-SPAM, and “Do Not Call” statutes. Legal requirements may apply based on characteristics of the constituent group (e.g. location, age, student status); the method of communication (e.g. texting, email); and/or the reason or content of the communication (e.g. health information, financial information). Individuals and units planning to send a communication to a large number of recipients internationally should first consult with the Office of the Vice President and General Counsel to ensure compliance with the laws regulating privacy and electronic communications in those countries, (e.g. EU-GDPR) if any.
5. Individuals and units given access to constituent information pursuant to this policy must comply with other applicable university policies and practices governing the use, safeguarding, and retention of institutional data.
6. Constituent communications must, wherever possible, be sensitive to constituent preferences. However, the university retains the authority and ability to communicate essential messages to any and all constituents at the university’s discretion. The university or campus has the authority to control communications that are in violation of this policy and its stated goals or that are in violation of any compliance requirements.
7. This policy, including all procedures and required approvals, is to be adhered to regardless of media, system, service, or method of communication.

Reason For Policy

1. This policy is designed to maximize communication, effectiveness of communications, and responsiveness to institutional objectives and constituent needs by leveraging the university’s resources in the most efficient manner possible and to ensure compliance with applicable law.
2. Indiana University views constituent relationship management as a strategic business process that manages the University’s relationships with its constituents, including but not limited to students, faculty, staff, affiliates, research subjects, research sponsors, patients and/or the public at large from initial interactions through every stage of the relationship and results in:
    - Greater engagement that leads to increased pride, loyalty, and goodwill;
    - Increased participation in events, programs and fundraising;
    - Improved understanding, awareness, collaboration and respect;
    - More visits and applications from qualified prospects around the world;
    - Official communication
    - Growth in academic activities and hence improved success for Indiana University students;
    - Stronger relationships with constituents through personalized, relevant and meaningful communication.

Procedure

1. Procedures for constituent relationship communications are determined by constituency, and guidance for approved communications is available from the Data Steward for the particular constituency.
2. The list of Data Steward contacts is located here: https://datamanagement.iu.edu/governance/data-stewards/index.php.
3. The Office of the Vice President for Communications and Marketing maintains a list of additional university officials authorized to approve constituent communications. It is essential to obtain approvals for the appropriate unit prior to sending a communication. https://salesforce.communications.iu.edu/getting-started/crm-approvals/index.html
4. Any questions regarding the appropriate Data Steward or communication approvers for a given constituency should be directed to the Office of the Vice President for Communications and Marketing.

Definitions

CAN-SPAM: The federal Controlling the Assault of Non-Solicited Pornography and Marketing Act, which, among other things, establishes national standards governing the transmission of commercial email.

Constituent: Anyone with whom the university has a relationship and who has a stake in its success, including but not limited to prospective students, current students, faculty, staff, alumni, parents, donors and friends, community members, business leaders, grantors, government officials, and the media.
Data Steward: An individual or entity that has approved management responsibility for the production, development, maintenance, use, and security of particular institutional data.
"Do Not Call" Statutes: State and federal laws that allow individuals to block most telemarketing calls, "robo-calls" and, in some cases, text messages made to cell and land lines. Requirements vary from state to state.
Engagement Communication: A communication which engages the constituent in a manner that further develops the relationship the constituent has with the university.
FERPA: The federal Family Education Rights and Privacy Act, which, among other things, governs the conditions under which student records may be disclosed among university officials and to third parties.
HIPAA: The federal Health Insurance Portability and Accountability Act, which, among other things, governs how certain health information must be protected when it is stored, accessed, and shared. It provides specific privacy and security provisions that include physical, technical and administrative safeguards.
Official Communication: A communication to a constituent that is essential and/or mandatory and primarily intended to provide information to the constituent. Examples are a message announcing the results of a Trustee election or a message discussing what the university is doing to address a time-sensitive issue.

Operational Communication: A communication to a university employee or broad group(s) of university employees that is meant to convey information about conducting university operational business processes. Examples are: a message announcing upcoming budget construction or year-end financial activity, a message informing users of system tips and upgrade information, etc.

University: For purposes of this policy, all campuses, schools, departments, programs, centers, and all other entities that are affiliated with or formally associated with the university and engaged in official university constituent communications.

Sanctions

Violations of university policies, including the failure to avoid a prohibited activity or obtain required approvals, will be addressed in accordance with the university policies and procedures applicable to the individual and the circumstances (i.e., Human Resources for staff, campus Academic Affairs for faculty, campus Student Affairs for students, the Office of the Vice President and General Counsel, and/or appropriate law enforcement agencies).

Failure to comply with university policies may result in sanctions relating to the individual's use of information technology resources (such as suspension or termination of access, or removal of online material); to the individual's employment (up to and including termination of employment in accordance with applicable university policy); the individual's studies within the university (such as student discipline in accordance with applicable university policy); civil or criminal liability; or any combination of these.

Units in violation of this policy may face restrictions on the use of institutional data or university systems.

History

This policy was established in 2019.

Related Information

DM-01 Management of Institutional Data
IT-21 Use of Electronic Mail
HIPAA and Fundraising
USSS-06 Student Rights Under FERPA
USSS-05 Release of Student Information Policy
GR-01 Contact with Federal and State Government Officials
Mass Email Procedures
Constituent Communications Best Practices
Record Retention Guidelines