Gettysburg College Access to Electronic Information Policy

I. Introduction

Members of the Gettysburg College community rely on technology in multiple aspects of their work, teaching, research, study, and other activity. In doing so, they use electronic systems, networks, and devices that Gettysburg College owns, provides, or administers. Gettysburg College makes these systems available for the purpose of carrying out its various activities and educational purposes. To promote trust within the Gettysburg College community, the College aims to be transparent about its policy regarding the circumstances in which it may access User Electronic Information stored in or transmitted through these systems.

Gettysburg College endeavors to afford reasonable privacy for users of the Gettysburg College Network and systems, and does not access information created and/or stored by users except when there is a legitimate operational need to do so.

Purpose: This policy sets out guidelines and processes that apply when Gettysburg College seeks access to such electronic information, consonant with the College's interest in maintaining an environment in which free academic inquiry thrives. This policy is intended to establish internal standards and procedures governing such access by Gettysburg College; it is not meant to create rights in any individual to seek legal redress for action inconsistent with the policy.

Scope: This policy applies to all uses of the Gettysburg College Network by all students, faculty, administrators, staff, alumni, parents, friends of Gettysburg College, and any other users of the Gettysburg College Network or Gettysburg College Systems.

College Authority: By using the Gettysburg College Network, users are granting permission for authorized Gettysburg College personnel to monitor, review, and/or intercept electronic communications, electronic records and data, and user information (as further defined below). Access that is necessary to render services or to protect the property of the provider of the service is allowed under the Electronic Communications Privacy Act of 1986 (ECPA). Further, electronic mail and other forms of electronic communication are neither secure nor protected by the laws that apply to the United States Postal Service. Email, records, files, communications, generated metadata, voice mail, text messages, social media activity, and any other network activity created using, stored on, generated on, transmitted via, or received by the Gettysburg College Network are Gettysburg College property and are subject to review by authorized personnel designated by Gettysburg College.

The College reserves the right to gain access to otherwise private Gettysburg College Network correspondence or files maintained on the Gettysburg College Network. System administrators may also require access to otherwise private communications or files maintained on the Gettysburg College Network as part of regular system maintenance. An attempt will be made to notify the user of this access in advance whenever possible and appropriate. Such access may be governed by applicable Federal, state, and local laws.

Access is grounded on six important principles:

1. Access should occur only for a legitimate, important, and documented College purpose;
2. Access should be authorized by an appropriate and accountable person, as designated by this policy;
3. In general, notice should be given when User Electronic Information will be or has been accessed;
4. Access should be limited to the User Electronic Information needed to accomplish the purpose;
5. Sufficient records should be kept to facilitate appropriate review of, and compliance with, this policy; and
6. Access should be subject to ongoing, independent oversight by the Ethics and Integrity Committee which includes faculty and administrative representation.

Terminology: The following terms are used in this policy with the following meanings:

- "College systems" refers to all services, networks, and devices owned, provided, or administered by any unit of Gettysburg College, including but not limited to email services, Internet access, file servers, voice message services, storage devices and services, laptop and desktop computers, phones and other mobile devices, and usage and access logs.
- "Users" refers to Gettysburg faculty, others holding academic appointments at the College, students, staff, other employees, volunteers, and visitors who access any College system.
- "User Electronic Information," refers to the following items created by, belonging to, or otherwise associated with a user:

    (i) Documents and communications, including emails, voice mails and text messages, and their associated metadata, which are located in files and accounts associated with a particular user. For example, this would include all emails and their attachments in a user's inbox, sent items folder, or other email folders that are recognized as part of the account associated with that user, and all documents in that user account's document folders; and

    (ii) Information generated by automated processes triggered by that user's use of College systems, such as tracks of Internet use, logs of access to facilities, logs of connection to wireless access points on the campus network, and transactions in various dining facilities.

    (iii) User Electronic Information does not include (a) records regularly maintained by Gettysburg College in the ordinary course of business, such as personnel records or student academic records, or information provided by personnel in connection with regular College record-keeping; or (b) information as described in (ii), above, when accessed by Gettysburg College without identifying or seeking to identify any particular user; or (c) information as described in (ii), above, when summarized or categorized and integrated into the College's regularly maintained records.

II. Reasons for Access

Gettysburg College does not routinely monitor the content of User Electronic Information transmitted through or stored in its information systems. Gettysburg College may obtain access to User Electronic Information in some circumstances, but only for a legitimate and documented institutional purpose. The paragraphs below describe certain purposes for which Gettysburg College may access such information. While this list is expected to cover most instances of access, the list is not intended to be exhaustive. Gettysburg College may access User Electronic Information for comparable reasons that likewise advance a legitimate institutional purpose, as determined by a person designated to authorize access pursuant to this policy and subject to review by the oversight committee as described in Part VII.

Although this policy applies to the Electronic User Information of faculty, staff, and students alike, in evaluating the institutional purpose, the person designated to authorize access should in each case weigh not only the stated reasons for access but also the possible effect of access on College values such as academic freedom and internal trust and confidence.

System Protection, Maintenance, and Management: College systems require ongoing maintenance and inspection to ensure that they are operating properly; to protect against threats such as attacks, malware, and viruses; and to protect the integrity and security of information. College systems also require regular management, for example, in order to implement new software or other facilities. To do this work, Gettysburg College may scan or otherwise access User Electronic Information.

Business Continuity: User Electronic Information may be accessed for the purpose of ensuring continuity in business operations. This need can arise, for example, if an employee who typically has access to the files in question is unavailable due to illness or vacation.

Safety Matters: Gettysburg College may access User Electronic Information to address exigent situations presenting threats to the safety of the campus or to the life, health, or safety of any person.

Legal Process and Litigation: Gettysburg College may access User Electronic Information in connection with threatened or pending litigation, and to respond to lawful demands for information in law enforcement investigations, other government investigations, and legal processes.

Internal Investigations of Misconduct: Gettysburg College may access User Electronic Information in connection with investigations of misconduct by members of the Gettysburg College community, but only when the authorizing person, after weighing the need for access with other College values, has determined that such investigation would advance a legitimate institutional purpose and that there is a sufficient basis for seeking such access. As described in Part VII of this policy, all decisions to access User Electronic Information are subject to review by an Oversight Committee.

III. Authorization of Access

Access to User Electronic Information should be authorized by an appropriate person, as set forth below. In deciding whether to approve access, the authorizing person should consider whether effective alternative means to obtain the information are reasonably and timely available. In all cases, access must comply with applicable legal requirements. Authorization for access to User Electronic Information may be provided by the consent of the user. Other cases should be handled as follows:

- If the user is a faculty member or other holder of an academic appointment at Gettysburg College, the Provost or designee must authorize access.
- If the user is an employee other than a faculty member or any other type of user other than faculty member or student, the Executive Vice President or designee must authorize access.
- If the user is a student, the Dean of Students or designee must authorize access, unless the reason for access is to further the investigation of a possible honor code or academic integrity violation, in which case the Dean of Academic Advising must authorize access.
- If the user is a student, the Dean of Students or designee must authorize access unless the reason for access is to ensure the immediate well-being of a student in which case designated Department of Public Safety personnel must authorize access.
- Any authorization of access shall apply only to the particular situation and user or users. Any other instance of access must be separately authorized.
- No independent authorization is required for information technology personnel to conduct routine system protection, maintenance, or management purposes in accord with internal protocols and processes. Likewise, requests for access in connection with litigation, legal processes, or law enforcement investigations, or to preserve User Electronic Information for possible subsequent access in accordance with this policy, need no independent authorization if made by the College's attorneys.
- In exigent situations involving a threat to campus safety or the life, health, or safety of any person, access may be authorized by the Executive Vice President, Provost or Dean of Students. If emergency conditions do not allow for prior authorization, the matter shall be reported to the Executive Vice President as promptly as possible.
- For some requests to search User Electronic Information, it may not be possible to identify any particular user in advance. For example, requests for logs of access to a College facility (swipe card data) often are intended to find out who entered a facility during a particular period; in such cases, the requestor cannot identify a particular user or users because the goal of the search is to learn those identities. Such data requests may still be subject to one of the prior provisions of this Section II, for example, those relating to law enforcement investigations or emergencies. Otherwise, such data search requests must be authorized by the Provost, Executive Vice President or Dean of Students as specified above.

IV. Notice

When Gettysburg College intends to access User Electronic Information, notice ordinarily should be given to that user. All reasonable efforts should be made to give notice before the time of access, or as soon thereafter as reasonably possible.

- System protection, maintenance, and management — Individual notice is not required for ordinary system protection, maintenance, or management. Notice should be given if the access relates specifically to the activity of an individual user.
- Business continuity — Individual notice is not required for access to User Electronic Information for purposes of business continuity, in accordance with established College practice and the common understanding that individual notice in such cases is typically not practical.
- Legal restrictions — Individual notice is not required where Gettysburg College is subject to legal constraints on its ability to give notice.
- Emergencies and other extraordinary cases — Contemporaneous notice is not required in cases where there is insufficient time, where giving notice would otherwise interfere with an effective response to an emergency or other compelling need (e.g., at a stage of an internal investigation where giving notice may compromise the investigation), or where it is impractical (e.g., in the case of a former employee). The decision not to give contemporaneous notice must be made by the person designated by this policy to authorize the access. In such cases, notice will ordinarily be given as soon as practical.

The person designated by this policy to authorize access may decide not to give notice. Any such decision, and the reasons for it, shall be described in the records described in Part VI of this policy and may be reviewed by the oversight committee, as set forth in Part VII.

V. Scope of Access

Gettysburg College shall adopt reasonable steps, whenever practicable, to limit access obtained under this policy to User Electronic Information that is related to Gettysburg College's purpose in obtaining access. These steps will vary depending on the circumstances of the search and may include, by way of illustration, designing searches to find specifically designated items, as opposed to categories of information. Participation in the search, and access to the information, should be limited to those personnel with a reasonable need to be involved.

VI. Records of Process

Any person who authorizes access to User Electronic Information shall provide that reasonable records of the decision process and the reasons for the decision are made in writing and preserved. The persons who implement access to User Electronic Information shall make reasonable written records and logs of the steps taken to access the information. All implementation records shall be delivered to and preserved by Gettysburg College's Vice President for Information Technology for a period of four years, after which they are to be deleted. Copies of the information accessed should be retained as needed to effectuate the purposes of the access. The accessed information and the records and logs of the search shall be

kept appropriately secure. In all instances of access under this policy, records adequate to permit effective review as described in Part VII of this policy should be kept.

VII. Oversight Committee

This policy, its implementation, and instances of access under this policy shall be subject to review by the Ethics and Integrity Committee. The Ethics and Integrity Committee shall make recommendations to the President as to the implementation of the policy and possible amendments. The Ethics and Integrity Committee shall also make periodic public reports on the implementation of this policy. In carrying out its responsibilities, the Ethics and Integrity Committee may review the records described in Part VI of this policy, subject to redaction as necessary to protect individual users.