# Frequently Asked Questions

The Policy on Access to Electronic Information ("AEI policy") cannot provide explicit descriptions of every eventuality. This document provides some discussion of the policy and additional examples to help community members understand how the policy might apply in a given situation.

Frequently Asked Questions

SECTION 1: User Electronic Information (UEI)

SECTION 2: Authorization to Access User Electronic Information

SECTION 3: Monitoring of UEI

SECTION 4: Scope of the AEI Policy

## SECTION 1: User Electronic Information (UEI)

**Q1. What is user electronic information, and what are some examples?**

User electronic information, or UEI, consists of (i) information generated by, created or received, on University systems that is located in accounts associated with a particular user; and (ii) information generated by automated processes triggered by that user's activity on University systems. Examples of UEI include documents in a user's document folder, emails in a user's University email account, and information generated through a user's interaction with University systems, such as card-swipe data (*i.e.*, building access logs) and log information generated by interacting with University networks, including Wi-Fi access points.

**Q2. What is <u>not</u> user electronic information, and what are some examples?**

UEI does not include footage or recordings made by Harvard-installed surveillance cameras, access to which is governed by Harvard's Policy on Installation and Use of Video Cameras.

Data or communications that include information about a user of University systems are not necessarily that user's UEI. As an example, consider the case where User A writes an email message to User B that includes information about User C. If Harvard proposes to access User A's email account to access that message, it can do so with User A's consent. Likewise, Harvard might obtain

User B's consent to access the message received from User A through User B's email. But because the message is not stored in User C's email account and was not auto-generated as a result of User C's use of University systems, the message--including what was said about User C--is not User C's UEI under the Policy. User C therefore cannot consent to Harvard's access to the message.

As another example, consider a case where a human resource officer assembles salary information for all the employees of a department and stores that information in her OneDrive account. This information is the HR officer's UEI, but not the UEI of any of the employees whose salary information is stored on OneDrive.

## Q3. Is all electronic information in any computer system subject to this policy?

No, only information held in University systems is subject to the AEI policy. Note that "University systems" are defined to be services, networks, and devices owned, provided, or administered by any unit of the University.

For example, information held by YouTube or some other third-party provider is not subject to the AEI policy if the University has not engaged the third party to provide services that include storing the information, as it is not information on a University system. By contrast, if the University has entered into a service agreement with an IT vendor to provide user accounts to members of the Harvard community, the data stored in those user accounts is subject to the AEI policy, whether the data are located on the vendor’s servers or stored on Harvard-owned or -administered servers.

Also, as noted in the policy, the policy does not limit or restrict access to records regularly maintained by the University in the ordinary course of business, or information generated by automated processes when accessed by the University without identifying or seeking to identify any particular user. Records stored in a Harvard archival repository are also not covered by the AEI policy.

## Q4. Is all electronic information generated by a user subject to this policy?

No, UEI includes only information generated from use of systems offered to users in their capacity as Harvard faculty, others holding academic appointments at Harvard, students, staff, and other employees.

Information generated by a Harvard community member when they are acting as a member of the public (for example, in the course of accessing the University's public Wi-Fi network from a personal device, purchasing tickets to a public Harvard event, or accessing a Harvard-administered website made broadly available to members of the general public) is not covered by the AEI policy.

However, all emails (whether personal or otherwise) sent by a Harvard faculty member using the University-provided email service are subject to the AEI policy, as the email service is provided to them in their capacity as a Harvard faculty member.

## Q5. What counts as "normal functionality and purpose of a University system"?

The AEI policy does not limit or restrict access to UEI that is part of the normal functionality and purpose of a University system.

For example, a shared email account provisioned to multiple users may be accessed by each such individual user in the ordinary course, and that access is not subject to the limits and conditions of the AEI policy. More generally, if a system is designed and intended to allow a team member to access the accounts of other team members to provide coverage in their absence, then such access does not fall under the AEI policy.

Another example is the Canvas learning management systems, which allows instructors to view student activity as part of the normal functionality of the system, for the purpose of understanding student engagement. An instructor’s use of this design feature does not fall under the AEI policy.

Yet another example is a messaging system that allows persons acting in a moderator role to review messages before they post, to ensure they meet the purpose and requirements of the system, or comply with standards for the platform. So long as the moderation is aligned with the purpose of the system and the expectations of the users and is part of the standard functionality and purpose of the system, then such access does not fall under the AEI policy.

A system may provide some functionality for system administrators to search, view, collect, or export information from individual users’ accounts. Such

functionality is typically exceptional: it is not part of the normal functionality or purpose of the systems and is therefore covered by the AEI policy.

## SECTION 2: Authorization to Access User Electronic Information

### Q6. Does every access to UEI require authorization?

No, the AEI policy explicitly excludes some information and access to information from the authorization requirement.

The AEI policy does not limit or restrict access to (or use or disclosure of) user electronic information that is part of the normal functionality and purpose of a University system. (See above for more information about what this means.)

The AEI policy does not limit or restrict access to “Log Information” (i.e., information generated by a user's interaction with University systems, such as building access logs) when that information is accessed without identifying or seeking to identify a particular user. For example, using building access logs to understand how busy a building is overnight does not identify or seek to identify particular users and so that access, use, and disclosure is not limited or restricted by the AEI policy.

The AEI policy does not limit or restrict access to UEI after it has been transferred into Harvard archival repositories; access to that information within those repositories is governed instead by the policies and practices of the Harvard University Archives.

In addition, the AEI policy does not require independent authorization for access provided under certain limited circumstances, including: access required for routine system protection, maintenance, and management; access required in connection with threatened or pending litigation, law enforcement investigations, or other government investigations; access to identify and disclose information as required by law or legal process (*e.g.*, a court order or subpoena); access expressly granted in a legal agreement, Certificate of Gift, or other stewardship agreement; and access by Harvard University Archives staff to determine whether records should be transferred to a Harvard archival repository.

In situations involving a threat to campus safety or the life, health or safety of any person where conditions do not allow for prior access to be authorized by the Chief of Police of Harvard University (or their designees), access does not need

prior authorization but must be reported to the Executive Vice President as promptly as possible thereafter.

## Q7. What authorization is required for accesses related to legal processes and litigation?

Section I of the AEI policy provides four reasons for access to UEI related to legal processes and litigation: (1) in connection with threatened or pending litigation, law enforcement investigations, or other government investigations; (2) to identify and disclose information as required by law or legal process; (3) to investigate or assist in the investigation of unlawful activity directed at the University or a member of the Harvard community, or (4) to investigate or assist in the investigation of unlawful activity by a member of the Harvard faculty or staff or other Harvard employee.

Requests for access related to (1) and (2) made by the Office of the General Counsel do not require independent authorization.

Requests for access related to (3) and (4) require the authorization of the General Counsel (or their designees). As in other cases where the AEI policy requires authorization, records of the decision to authorize, including the process and reasons why, must be made, preserved, and provided upon request to the Electronic Communications Policy Oversight Committee (ECPOC) to review.

## Q8. What constitutes a user's consent to access?

Authorization for access to UEI may be provided by the consent of the user. “Consent” refers to the permission of a user to access the user’s UEI following a clear and specific description of the purpose and the extent of the access requested.

## Q9. Does the AEI policy permit a family member of a deceased Harvard affiliate to access the affiliate's user information?

The AEI policy applies to UEI even after the death of the Harvard user. In cases where a family member provides legal documentation sufficient to establish that the requester is acting on behalf of the deceased user’s estate, the University may determine that the family member is acting “as” the user, such that the AEI policy would not restrict access to the user’s UEI.

# SECTION 3: Monitoring of UEI

## Q10. What monitoring of information transmitted through or stored in University information systems happens?

The content of information transmitted through or stored in University systems is not routinely monitored by humans, including Harvard personnel or others. However, automated processes do routinely monitor such information, for the purposes of routine system protection, maintenance, or management purposes.

## Q11. What counts as "routine system protection, maintenance, or management purposes"?

The AEI policy does not require independent authorization for routine system protection, maintenance, or management purposes.

Routine system protection may involve the automated scanning of UEI. For example, automated tools might check that publicly available documents or outgoing emails do not contain potentially sensitive information such as Social Security numbers, credit card numbers, or other forms of personal information that if left unsecured could cause harm to individual persons, and might provide automated warnings or messages to the relevant users. Tools might embargo outgoing email or restrict access to documents until reviewed by the relevant users.

Automated tools may also scan inbound electronic communications to screen out spam and phishing messages, and messages containing malware.

Routine system protection also includes investigation of and response to computer security incidents, such as investigating whether an account has been compromised and what data or systems were accessed by an intruder. These actions do not require independent authorization, but notice should be given if the investigation of a security incident relates specifically to the activity of an individual user. However, notice is not generally required in incident investigation or response if the UEI that is accessed is incidental to the investigation.

Security incident investigation and response may also require searches to determine which users have received potentially dangerous emails, such as phishing attacks or malware. Protecting the system may necessitate the removal

of such emails from users' email accounts. However, note that this applies only to clearly identifiable threats; non-automated searches for hate speech, misinformation, or other questionable content should require authorization in accordance with the AEI policy.

## SECTION 4: Scope of the AEI Policy

### Q12. Are video recordings covered under this policy?

This policy does not cover access to data from video cameras operated on the Harvard campus for safety, security and facilities management purposes. The information recorded by video cameras is not "user electronic information." Use of that data falls under the Policy on Installation and Use of Video Cameras. Please visit the Policies page on the Provost's Office website for a list of all University-wide policies.