University of Colorado
Boulder | Colorado Springs | Denver | Anschutz Medical Campus

OFFICE OF ADVANCEMENT

CU Advancement Data Sharing Policy for Employees and Volunteers

Introduction

This document provides employees and volunteers of the University of Colorado Office of Advancement with principles for data sharing to safeguard the interests of our organization, employees, volunteers, and donors. Protecting the relationships we create with our supporters is a top priority, as our work often involves confidential information. These guidelines build upon established policies and offer specific instructions for managing sensitive data.

Discretion in sharing data outside of Advancement is crucial. There are situations where sharing requested data should not occur. Understanding the business needs and purpose for the data is paramount before sharing any data outside of Advancement. Advancement staff should consult with their managers regarding questions or concerns about sharing data outside of Advancement. You can also email Advancement.Help@cu.edu with any other questions.

General Principles

All employees and volunteers of the University of Colorado are responsible for following the established policies and standard operating procedures regarding the appropriate use of confidential, proprietary, and highly sensitive information with the goal of protecting the privacy of our constituents.

Multiple laws may apply to donor data including but not limited to

- Family Education Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- General Data Protection Regulation (GDPR)

We abide by:

- CU Privacy Policy
- CU campus privacy statements

○ CU Boulder

○ CU Denver/Anschutz ○

UCCS

We are further guided by ethical policies and guidelines of relevant professional associations, notably:

- AFP Code of Ethical Standards
- APRA Statement of Ethics
- AFP Donor Bill of Rights

Data gathered and maintained by employees, volunteers, or consultants of the University of Colorado is considered institutional data. The University of Colorado owns institutional data, and each authorized user is responsible and held accountable for its appropriate and authorized use.

Data Usage Restrictions

Use of donor data for purposes other than for Institutional Advancement, especially for commercial, personal, or political purposes, including the sale of data, is strictly prohibited. Advancement purposes include engagement, cultivation, and solicitation.

Information maintained in hard copy or electronic files as part of an official university record shall be viewed only by authorized University of Colorado employees and representatives (including selected volunteers) who need such information for legitimate institutional advancement business.

Data shared outside of the Advancement Division must be stored within CU Ascend, and any shared documents must be shredded. Sharing data with consultants is prohibited unless there is a legal agreement approved by relevant Advancement leadership. Only the minimally needed confidential information should be provided by Advancement staff to non-Advancement staff and volunteers**.**

Failure to Comply

Non-compliance with this policy will result in notification to the appropriate executive leadership and may lead to loss of access to advancement data. In severe cases, it may also result in disciplinary action, up to and including termination of employment.

Definitions

Please refer to The University of Colorado Anschutz's Regulatory Compliance for full definitions

Highly Confidential Information – This category includes data elements that require protection under laws, regulations, contracts, relevant legal agreements and/or require the institution to provide notification of unauthorized disclosure/security incidents to affected individuals, government agencies or media. Advancement related highly confidential items includes things like:

- Protected health information
- Social security numbers
- Payment card numbers
- Financial account numbers: including university account numbers, student account numbers, and faculty and staff direct deposit account numbers
- Driver's license numbers
- Health insurance policy ID numbers
- Level 4 and 5 of Student Data (SSN, NID, Financial Aid (except work study), loan and bank account numbers, health information, disability, race, ethnicity, citizenship, legal presence, visas, religion, sexual orientation, sex at birth)

Confidential Information – This category includes data elements not usually disclosed to the public but are less sensitive than Highly Confidential data. If a legally required and applicable Colorado Open Records Act (CORA) request is submitted, these records may be released. Advancement related confidential items includes things like:

- Contents of project files, strategic plans, terms, and conditions of gift agreements completed or under negotiation
- Donor information such as appraisals and giving histories
- Any donor or fundraising strategy information that would pose a problem to CU where it accessed by unauthorized individuals through a breach of data security is considered confidential. Donor contact information and non-public gift amounts, including but not limited to:
    - Records of gifts that a donor wishes to be publicly anonymous
    - Any document mentioning a specific gift or range of gifts connected to a donor or group of donors not approved for public release
- Fundraising information
- Non-public policies
- University and employee ID numbers
- Internal memos and email, and non-public reports
- Proprietary information limited to authorized employees and selected volunteers of CU. Examples of Proprietary information would include:
    - Fundraising status reports that do not include specific donor names o

      Fundraising activity reports
    - Information about specific programs that does not include discussion of specific donor strategies

Donor/alumni names and contact information are considered confidential and cannot be shared for non-Advancement purposes. When donors and alumni wish to contact each other, no information can be released to the inquiring person. Instead contact information can be collected from the inquiring person and shared with the person being inquired after.

Public Information – Information is considered public when the University of Colorado does not place limits on media in which it may appear or the persons who may have access to it. Advancement related public items includes things like:

- Donor names with designated gift levels to be published in any form of annual report and/or posted on CU web sites. (excluding anonymous)
- Donor-approved press releases, announcing specific gifts
- Information about donors who provide named funds shared in materials about programs their funds support. In general, only information the University of Colorado chooses to make public for recognizing contributions and\or attracting similar support from other potential donors will be considered public. Even data gathered from public sources, such as wealth screening information, which is then converted to CU donor data, shall be treated as confidential

CU Advancement Data Sharing Policy Addendum

I have read the Data Sharing Policy and now what can I share? Please find some examples below. As a reminder from the Data Sharing Policy Document, “only the minimally needed confidential information should be provided by Advancement staff to non-Advancement staff and volunteers.”

For more information on acceptable methods and tools for transmitting or storing of institutional data, contact Advancement IT at Advancement.Help@cu.edu.

1. Sharing Information with Volunteers

Sharing information with volunteers can be appropriate when Advancement staff have determined that an Advancement task is best completed by volunteers, and that the volunteers need certain data to complete the task.

- Example 1a: If volunteers are calling donors and alumni to invite them to an event, share the required information such as phone number, name and state/city. Do not share email, giving levels and addresses.

- Example 1b: If a School’s Board is responsible to reach out to their fellow cohort to solicit gifts and update them about the School, provide them with a yes or no to whether their peers have given this year, along with the name, class year, and appropriate contact info.

2. Sharing Information with Individuals Who Are Not Employees or Volunteers

When those requesting information are not CU staff or volunteers, but rather alumni, students, family of donors, etc., then information should generally not be directly shared. Instead, an Advancement staff member can act as an intermediary.

- Example 2a: If an alumnus contacts you to share information about a classmate, collect the inquiring person’s contact information and share it with the person being inquired after.

- Example 2b: If a gift was made in honor or in memory of an individual and that individual’s family would like to thank the donors, connect with the donor and ask if it is alright to share their contact information with family. If approved, provide name and contact information only, not gift amounts.

- Example 2c: If a scholarship recipient wants to send a thank you letter to their donor, act as an intermediary. The student can write the letter, give it to Advancement staff, and Advancement staff can send it.

3. Sharing Information Covered by Other Policies

Some information or requests are covered by laws or regulations that would supersede this policy.

- Example 3a: If a donor requests information we store about the personally (i.e. contact reports), direct inquiries to privacy@cu.edu. If requested, provide contact information we store about them, but not personal details about others.

- Example 3b: If Channel 9 News requests information about CU, say nothing and connect them with CU's Vice President of Communications.
- Example 3c: If HIPAA or Protected Health Information (PHI) data needs to be transmitted to another CU advancement staff member, consultant or affiliate, use the Advancement GP Shared Drive. Do not send HIPAA data through email. If you need access to this shared drive, you will need to pass the required Skillsoft HIPAA training course and reach out to Advancement.Help@cu.edu for access.

4. Sharing Information for Non-Advancement Purposes

Act as an intermediary for non-advancement purposes.

- Example 4a: If a CU staff member wants a list of alumni for a gala, advancement staff can send the invitations the staff member drafted.
- **Example 4b: If a CU Advancement staff member wants to use advancement data for their CU masters or doctorate thesis,** discuss the request with System Advancement Leadership Team. Provide details on the data needed, how it will be used, and how it will be securely stored.
- **Example 4c: A CU staff member wants to access advancement data for mass email blast,** Advancement staff can refuse to act as an intermediary if the request does not meet a specific business need or if other priorities would restrict them from fulfillment. Determine the business need and discuss with the System Advancement Leadership Team and/or IT Security.

5. Sharing Information with 3rd Party Applications and Vendors

Third-party consultants or vendors engaged by Advancement or Foundation may only access data after appropriate contracts or legal agreements are established and approved by Advancement leadership (Campus Vice Chancellors, System Vice President for Advancement Administration, and CU Foundation President & CEO).

- Example 5a: If advancement data for advancement purposes needs to be stored in a third-party application, SAAS, or Cloud environment, contact Advancement IT who will work with the Advancement Data and Technology Council (ADTC) to determine if an MOU is required. Further discussion with System Advancement Leadership team may be needed. A Business Associate Agreement may also be required if HIPAA or Protected Health Information (PHI) data is utilized.

- **Example 5b: If advancement data and/or access to Ascend and AI is requested for third-party vendors or consultants that have been procured by CU Advancement and the CU Foundation,** ensure appropriate contracts or legal agreements are established and approved by the relevant leadership. Both System Advancement leadership, CU Foundation and the appropriate campus leadership must be involved in reviewing and approving the vendor's proposed use of institutional data. The following must be assessed and clearly documented in the contract:
  - The specific data the vendor will require
  - The duration for which data will be stored with the vendor
  - The vendor's security procedures for handling data
  - How any data generated by the vendor for Advancement staff will be managed

Revision

This policy will be reviewed annually or as needed to ensure its effectiveness and alignment with changing business requirements and regulatory obligations. Any proposed revisions to the policy should be submitted to the Advancement Security team for review and approval.

Relevant Documents

- CU Privacy Policy
- AFP Code of Ethical Standards
- APRA Statement of Ethics
- AFP Donor Bill of Rights
- Regulatory Compliance

Addendums and Change Log

Addendums

Change Log

>> If changes to the above guidelines are made and approved, add the date of adoption followed a brief description of the change as a bulleted list below.

- **[07/18/2025]** – Policy Change log added and Example 4c edited
- **[08/05/2025]** – Example 3c Updated per Jerry Sinning

Originally Approved:	04/17/2025
Officer:	Chris Rose
Review Cycle:	Annual
Reviewed:	[Dates]
Revised:	[Dates]