Policy Name	Data Use Policy		
Policy #	6.1	Effective Date	February 20, 2026
Responsible Department	CUF IT	Cross Reference	6.1P
Approved by	Data Governance Executive Council, CUF Senior Staff	Policy Owner:	Executive Director of IT

Clemson University Advancement - Data Use Policy

(Guidelines for Data Consumers, including Confidentiality and Anonymity)

1. PURPOSE

Clemson University Advancement is committed to safeguarding the privacy and confidentiality of information entrusted to the University by students, alumni, parents, donors, staff, volunteers, and prospects. This policy establishes standards for the appropriate access, use, and protection of Advancement data to ensure compliance with legal, regulatory, contractual, and University requirements.

2. DEFINITIONS

- **Data Consumer**: Any individual (employee, affiliate, volunteer, or vendor) granted access to Advancement data.
- **Advancement**: The division of Clemson University that includes the Clemson University Foundation, Development teams/units, Clemson Alumni Association, and IPTAY.
- **Data Access Manager**: An Advancement employee responsible for authorizing, monitoring, and managing data access for Data Consumers under their supervision.

3. SCOPE

This policy applies to Clemson University employees inside and outside of the Division of Advancement, vendors, affiliates, and volunteers who request access to data for communication, solicitation, research, analysis, and/or reporting.

This policy shall also govern user access obtained through any affiliation agreement, service level agreement, or data collaboration agreement between the Clemson University Foundation and Clemson University or any of Clemson University's affiliated entities, including IPTAY, the Clemson Alumni Association, and the Clemson Architectural Foundation.

4. DATA CLASSIFICATION

The University, in alignment with the State of South Carolina, has adopted four data classification categories: Public, Internal Use, Confidential, and Restricted. These classifications are defined below. The categorization of data will determine what security controls are required for related systems and applications.

Public

- Data is developed and intended for public disclosure.

Internal Use

- Data is not Confidential or Restricted, but not generally available to the public.
- A breach of confidentiality, integrity, or availability could have minimal adverse impact on the University's mission, safety, finances, or reputation.
- The information pertains to or is used in the daily operations of the University.

Confidential

- The information is sensitive and is to be kept protected as a matter of University policy, procedures or contractual obligation.
- A breach of confidentiality, integrity, or availability could have an adverse impact on the University's mission, safety, finances, or reputation.

Restricted

- The information is highly sensitive and is to be kept protected as a matter of law, regulation, and contractual obligation.
- A breach of confidentiality, integrity, or availability could have a significant adverse impact on the University's mission, safety, finances, or reputation.
- The University is subject to statutory or regulatory penalties or notification provisions in the event of any unauthorized access or disclosure.

The Example Data Elements table below contains a list of commonly used data types across campus.

Public	Internal Use	Confidential	Restricted
- Public facing websites - Policies and procedures designed for public use - Published research data - University contact information not designated by the owner as private - CUID (XID)	- Non-public policies - Training materials - Unpublished research data - Non-public contracts - Contracts, emails, memos, budgets, reports, or policies distributed only within Clemson	- Donor contact and non-public gift information - HR records - Birth date, addresses, personal contacts and other Personally Identifiable Information (PII) - Survey data collected which includes identifiers - FERPA protected data	- Controlled Unclassified Information (CUI) - Protected Health Information (PHI) - Federal tax info received or derived from the IRS - Individual financial aid information subject to Gramm-Leach-Bliley Act - SSN - Debit, credit card numbers, - Bank accounts

Specific examples in Advancement:

Public	Internal Use	Confidential	Restricted
- Donor recognition (without specific dollar amounts) - Online Honor Roll	- FYFRS (financial report) - Engagement metrics - Donor names with designations and amounts	- Prospect Reports and ratings - Anonymous donor information	- Original or scanned check - Donor's Last Will & Testament

5. DATA CONSUMER CLASSIFICATION

1. **Advancement Employees**: Staff members employed by Advancement, granted role-based access to Advancement systems as required by job function.

2. **University Partners** (Auxiliary and Non-Auxiliary): Must be requested by, assigned to, and managed by a Data Access Manager. Each Data Consumer will receive data commensurate with job function**.**

a. Auxiliary Users

Non-Advancement employees who are assigned an account into CADENCE to self-serve, for data approved by the Data Governance Council.

This limited group is specifically defined by the DGC in the procedural documentation. **b.**

Non-Auxiliary Users

A larger group that receive data generated and published by Advancement Staff. (No account/direct access to CADENCE application). Requests are approved in accordance with Data Governance Council guidelines and aligned with the relevant role. For example, business officers use revenue data for budgeting, and stewardship liaisons in the colleges/units use data for sending correspondence.)

3. **Volunteers:** Must be requested by, assigned to, and managed by a Data Access Manager. Each Data Consumer will receive data commensurate with the volunteer's role (ie. Class Reunion Chair, Campaign Cabinet Member).

4. **Vendors:** Third parties granted access only after meeting vendor management, security, and nondisclosure requirements established by the Clemson University Foundation Management Policy and Procedures. A non-disclosure agreement should be signed either as part of the contract or as a separate document.

6. POLICY

6.1 Appropriate Use

All Data Consumers with access to fundraising data are responsible for data security and privacy for any data extracted from the fundraising systems.

- Data Consumers must access, use, share, and purge data only as authorized and in alignment with their University responsibilities and policies: www.clemson.edu/ccit/cybersecurity/policy/
- Confidential and Restricted data must be stored, transmitted, and shared only through University approved secure systems.
- Personal, commercial, or unauthorized use of Advancement data is strictly prohibited.

6.2 Solicit Codes

Solicit code and anonymity notations on constituent records (listed below) determine how constituents can be communicated.

- Donors have control over their solicitation and confidentiality setting. If a donor indicates that they prefer one form of communication over another or if they indicate that they want their gift or record marked confidential, then their direction must be followed by all Data Consumers.
- Data Consumers must comply with donor solicitation codes and anonymity requests (e.g., "Do Not Contact," "Anonymous Giver").
- Exceptions require documented approval from Advancement's Executive Committee of the Data Governance Council (DGC) or designee.
- In accordance with GDPR requirements, all EU residents are defaulted to "Do Not Contact Except Mandatory", and cannot be changed without explicit written consent. Clemson University GDPR program details are available here: https://www.clemson.edu/administration/compliance/privacyprogram/gdpr.html

Solicit Code	Description
Do Not Contact Except Mandatory	Do not contact constituent at all (via any communication method) except for mandatory communication which includes gift receipts and endowment statements. Any other communication considered "mandatory" must be pre-approved as described in the policy
No Postal Mail	Do not send any postal mail to constituent
No Marketing of Products or Services	Do not send any marketing communication for products or services (via any communication method) to constituent
No Solicitation	Do not solicit constituent (via any communication method)
No Postal Solicitation	Do not send any postal mail solicitations to constituent
No Phone Calls	Do not call constituent
Omit from Call Lists	Do not include constituent in any mass phone lists
No Email	Do not email constituent
No Text/SMS	Do not text constituent

6.3 Types of Anonymity

1. **Individual Gift** – a specific gift may be marked anonymous.
2. **All Giving** – a donor's record is marked that all gifts made by the donor are made anonymously.
3. **Giving Recognition Category** – a donor may request that their giving recognition category is kept anonymous.

6.4 Roles and Responsibilities

1. All Data Consumers must sign the Data Use Policy annually.
    - Data Consumers must complete onboarding training prior to receiving access.
    - Access to the fundraising database and other data systems will be managed by CUF based on the role and job function the employee performs at/for the University.
    - Supervisors/Data Access Managers are responsible for requesting access, updates to access and termination of access, and for ensuring role-appropriate training and compliance.
    - All accounts must be terminated immediately after a Data Consumer has ended their relationship with CUF (employment, volunteer role, etc.)

6.5 Data Retention and Disposal

- Information must be disposed of in accordance with any applicable University policy that may apply to the data and be securely shredded, deleted, or otherwise disposed of in a permanent and complete fashion.
- Clemson University's Record Retention Schedule: https://libraries.clemson.edu/recordsmanagement/retention-schedules/

7. COMPLIANCE & ENFORCEMENT

- The Clemson University Foundation and the Division of Advancement is responsible for ensuring data security and may audit Data Consumer activity.
- Suspected or confirmed breaches must be reported immediately in accordance with the University's Data Breach Response Policy: Data Breach Response Policy
- Advancement's Data Governance Council Executive Committee, through recommendations from appointed Data Stewards and the Data Governance Council, evaluates, updates, and/or upholds data policies and procedures in alignment with University Data Governance.
- Data Consumers that violate this policy will have access to constituent information and communication with constituents suspended either temporarily or permanently, and the matter will be turned over to the University.
- Violations may result in termination of access, reporting to institutional authorities, and legal consequences.

Affirmation for Data Consumers:
I have reviewed the Data Use Policy for Clemson University Advancement, and I agree to abide by its terms and conditions.

Approved by the Data Governance Executive Council & CUF Senior Staff
February 20, 2026

SCAN ME