High-Level Process - Advancement Data Sharing Process

Parent Policy: Advancement Data Sharing Policy

Contents

1.0 Purpose and Scope 1
2.0 Process and Procedures 1
2.1 Process Requirements 2
2.1.1 Data Collection and Usage 2
2.1.2 Systems, Maintenance and Storage 2
2.1.3 Sharing 3
2.1.4 Record keeping 4
3.0 Roles and Responsibilities 4
4.0 Compliance and Review 5
4.1 Compliance 5
4.2 Acceptable Use 6

1.0 Purpose and Scope

This high-level process supports the implementation of the Advancement Data Sharing Policy. The policy applies to all members of the University of San Francisco (USF) community, both internal and external, and includes but is not limited to students, faculty, staff, affiliates, contractors, and volunteers in all locations, both on- and off-campus, that access, manage, and use information and data about Advancement constituents.

This process covers the collection, access, maintenance, storage, and use of information and data about Advancement constituents. Following this process ensures USF's compliance with privacy laws and

regulations and promotes the responsible use of the information and data to maintain positive relationships and foster engagement for Advancement constituents.

2.0 Process and Procedure

Advancement will develop, implement, and maintain practices and procedures to facilitate Advancement personnel, and any others granted access by Advancement, to securely and appropriately use and protect the privacy and confidentiality of the information and data about Advancement constituents.

2.1 Process Requirements

Users with access to the information and data about Advancement constituents must comply with the key aspects of the Data Sharing Policy to:

- manage and safeguard the information and data about the Advancement constituents and associated technology assets;
- manage and grant access to the information and data to members of the University community, internal users, and approved external parties; and
- ensure the Advancement constituents' privacy is respected and protected.

2.1.1 Systems, Maintenance, and Storage

The University's primary database of record-holding information and data on Advancement constituents is currently AdvancementRM, previously known as Affinaquest (and generally referred to internally as "AQ"). This database application is hosted externally by Salesforce. The associated processes and procedures needed to secure, safeguard, maintain, and manage AQ are jointly owned by Advancement and ITS.

All personnel who want to communicate with Advancement constituents or use the information and data for Advancement and alumni relations purposes *must* liaise through existing channels with Advancement. Advancement uses AQ as the primary data source along with approved tools that integrate with AQ.

2.1.2 Data Collection and Usage

USF collects and maintains information and data about Advancement constituents from a variety of sources:

- alumni information collected when an individual initially enrolls as a student at USF and then unenrolls or graduates;
- Advancement data gathered after the alumni is no longer enrolled as a student; and

- donor information about a donor or prospective donor collected by Advancement or any college, school, department, or unit within USF, or any other University employee for Advancement and related purposes.

This information and data about Advancement constituents is used in developing and nurturing relationships between the constituents and the University to achieve the goals and objectives set forth by the University.

2.1.3 Sharing

Constituent information and data are considered confidential and generally not disseminated. Advancement is responsible for managing the procedures to grant and revoke access to the information and data. All data and reports obtained under this access are confidential, for the purpose set forth, and for the exclusive use of authorized USF internal users, external parties, and volunteers.

a) Internal Sharing

Only University individuals authorized by Advancement, and who have a need-to-know business purpose to perform an authorized University function or activity, may have access to constituent information. Alumni and donor information shall be used solely for USF's Advancement purposes in accordance with applicable Advancement and University policies.

Alumni information may be shared internally among authorized staff members strictly for alumni-related purposes.

1. An individual may access information and data about Advancement constituents after Advancement has determined that they have an appropriate, necessary, and clearly defined purpose for data use and they are acting as an agent, representative, or contractor of USF for that purpose.

2. Access to Advancement constituent information and data is not necessary to schedule communications, such as an alumni newsletter. Communications processes are in place to support these efforts without requiring internal users to receive access to AQ and/or individual data lists. See the *Advancement Email Marketing Best Practices* for more details on established processes and resources available to internal users for communications with alumni, parents, donors, friends of USF, etc.

3. Advancement constituent information and data are not shared outside of Advancement. If an internal user wishes to email alumni, they may use the resources outlined above. If they wish to discuss stewardship, they may contact stewardship@usfca.edu to coordinate this effort while adhering to Advancement's data access and practices. In rare cases when transmitting

information outside of Advancement or via approved secure channels to the Office of Marketing and Communications, the sender will follow all standard operating procedures to protect constituent data. Recipients of data are responsible for using it only for the purpose outlined, and deleting the data immediately after using it for the approved purpose.

b) External Sharing

In certain select and approved cases, alumni & donor data may be shared with trusted third parties (e.g. mailing services, event organizers) and volunteers (e.g. alumni, USF Board of Trustees) only when necessary to fulfill donor and alumni-related activities. Such individuals and third parties are contractually bound to protect the confidentiality and security of the data. (Note: third-party vendors and service providers must be vetted and approved through ITS, OGC, and Risk Management *prior* to engagement.)

1. Volunteers - Departments within Advancement may release limited information to volunteers upon request as outlined below.
    a. Before releasing the information and data, they must request and receive permission from both AVP- Engagement and AVP-Advancement Operations and ensure the volunteers are aware of and have committed to following University policies on securing, storing and usage of the data.
    b. A signed volunteer confidentiality agreement is required and may be obtained by contacting Advancement. Signed volunteer confidentiality agreements are maintained securely by Engagement.
    c. Inquiries may be directed to giving@usfca.edu.
2. External parties - constituent data will only be shared with external parties for third-party marketing, commercial purposes, data analytics purposes, or other requested uses with the explicit consent from Advancement via the AVP-Advancement Operations.
    a. Alumni data used by non-internal users, i.e. any third party, including volunteers, must exclude the alumni's CWID, Salesforce/Affinaquest ID, and any data records coded as Confidential should not be included unless explicitly approved in writing by the AVP-Advancement Operations. If for the purpose of a communication, applicable contact exclusions will be honored as is standard with all communications requests.

2.1.4 Record Keeping and Contact Exclusions

The actions to maintain the currency and accuracy of the records in AQ are owned by Advancement. This includes adding new records and removing records as needed. Advancement shall maintain a record of all requests by individuals or entities who notify the University that they do not wish to be contacted by or on behalf of Advancement and/or USF. Upon receiving the request, Advancement and/or USF will discontinue further contacts, and the individual's or entity's record in AQ will be promptly updated to ensure no further contact is made.

3.0 Roles and Responsibilities

As the data steward of the information and data about Advancement constituents, the AVP-Advancement Operations is responsible for establishing, authorizing and maintaining the necessary roles and responsibilities to deliver the services Advancement needs including the support and maintenance of AQ.

Role	Responsibility	Skill/Knowledge
Assistant Vice President (AVP), Advancement Operations (AVP- Advancement Operations)	Data Steward of information and data about the Advancement constituents. Responsible for maintaining and authorizing and revoking access to, and the use of, the alumni and donor information and data. Responsible for inventorying the data, its classification, and application assets under Advancement's control, assessing the assets for risk, and understanding USF's degree of risk tolerance relating to alumni and donor data.	Advancement processes, operations, and goals. Relevant donor and alumni data protection laws and regulations and CASE industry standards.
Data Governance Committee	Support these processes. Review and provide guidance on data transfers to external third parties as applicable.	Institutional data definitions/glossary
Advancement staff in Advancement Operations vertical	Operate AQ's database administration services, maintain user security roles, set permissions and grant/revoke access rights, maintain system integrations, establish regular backup, and maintain the accuracy and currency of records in AQ.	User and systems knowledge of Salesforce and AQ. Advancement's Prospect Management Policy and Data Clearance Policy. Adhere to CASE industry standards.
Internal Users	Maintain the confidentiality, integrity, and availability (i.e.	Relevant Advancement policies: Alumni and Donor Privacy Statement;

	"CIA") of the data internal users access, use, and interact with.	Advancement's Prospect Management Policy; Advancement Data Clearance Policy; Advancement Email Marketing Best Practices; Complete required ITS and other University-assigned trainings.
External Parties	Maintain the confidentiality, integrity, and availability ("CIA") of the assets they access, use, and interact with.	
Associate Vice President and Director, Application Services	Provide technical- and back-end support for Advancement, and work with AdvancementRM product vendor when support issues require the vendor's assistance. As requested, support Advancement staff in database operations.	Technical knowledge of Salesforce and AQ including knowledge of when the asset is reaching the end of its life and what the potential retirement/replacement options may be.

4.0 Compliance and Review

This process is periodically reviewed and updated to reflect changes in data protection laws, organizational policies and practices, or technological advancements.

4.1 Compliance

As steward of Advancement constituent information and data, Advancement is committed to complying with all relevant data protection laws and regulations.

- Advancement is committed to keeping Student, Parent, Alumni, Donor, and Donor Prospect information safe and preventing misuse.
    - Advancement adheres to the University Prospect Management Policy, and guidelines and standards set forth by the Council for Support and Advancement of Education (CASE). The Advancement is responsible for maintaining membership(s) with CASE and making available copies of the standards for all Advancement staff (and any other affiliate by request).

    - All Advancement staff are required to uphold and adhere to all Advancement policies.
- Advancement ensures compliance by requiring all internal users requesting access to information and data about Advancement constituents to:
    - Complete ITS Information Security Awareness Training, ITS Elevated Access Training, and AdvancementRM ("AQ") database training before being granted access.
    - Adhere to Advancement's Data Clearance Policy, which is shared as part of standardized onboarding and is available in Advancement's policy repository

4.2 Acceptable Use

Information and data about the Advancement constituent shall be used only as allowed under this process. In addition, the information and data must *not* be:

- used to contact and/or solicit Advancement constituents without following the proper Advancement procedures and permissions.
- used to stalk or harass Advancement constituents.
- used to solicit for personal purposes or gain.
- used to solicit for institutions not affiliated with the University without proper authorization.
- sold for personal purposes or gain.
- used to trade, exchange, share, give, etc. the information and data to people or institutions not affiliated with the University without proper authorization. (Note: all third parties identified to receive the information and data must agree to safeguard such information and data in compliance with USF's policies prior to being engaged.)
- used to store or transmit Advancement constituent information and data on personally owned devices or via personally maintained services that are not managed by the University.
- used to store or create any type of stored data, database, or dataset outside of AQ that mirrors or uses information in AQ but is not integrated with AQ.
- used to any purpose other than the reason it was originally requested, reviewed, and approved for.

Failure to follow these processes as part of the overall Advancement Data Sharing Policy will result in disciplinary action and may include denial of current and future access to Advancement constituent information and data, and may potentially lead to termination and/or legal action.
