DAR data access

Policy Type: Local
Responsible Office: Office of Development and Alumni Relations
Initial Policy Approved: 12/2012
Current Revision Approved: 6/30/2021

Policy Statement and Purpose

The Office of Development and Alumni Relations collects and maintains confidential information to support philanthropy, marketing and engagement operations of the university. As the authoritative data source, DAR restricts access to constituent records, legal documents, and gift accounting records. Alumni, donor, and prospect reports are considered a protected asset required for the business operations of DAR, university development units, and affiliated foundation partners.

Personal Identifiable Information is only accessible for a university business need related to constituent communications, development and alumni relations. As data stewards, DAR determines the process, approval, and controls for access to the database of record.

DAR may authorize data sharing upon approval of the business need and completion of a required confidentiality protocol. Signing of the DAR Confidentiality Agreement does not guarantee access to the university’s donor database of record. Constituents may consent to the release of their own information, upon request.

This policy’s overarching objectives are to create a transparent system that protects donor, alumni and constituent data and respects the expectations and intentions of all parties, and to ensure that data management decisions do not conflict with the university’s values or best interests.

Noncompliance with this policy could result in disciplinary action up to and including termination. VCU supports an environment free from retaliation. Retaliation is prohibited against any employee who brings forth a good faith concern, asks a clarifying question, or participates in an investigation.

Table of Contents

<table>
<thead>
<tr>
<th>Who Should Know This Policy</th>
<th>#2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Definitions</td>
<td>#2</td>
</tr>
<tr>
<td>Contacts</td>
<td>#3</td>
</tr>
<tr>
<td>Policy Specifics and Procedures</td>
<td>#3</td>
</tr>
</tbody>
</table>

DAR Data Access 1 Approved: 6/30/2021
Who Should Know This Policy

All university employees engaged in activities related to development and alumni relations are responsible for knowing this policy and familiarizing themselves with its contents and provisions.

Definitions

Advancement Services records
Advancement Services’ records include all written papers, letters, documents, photographs, tapes, microfiche, digital copies, photocopies, sound recordings, maps and other documentary materials or information in any medium regardless of physical form or characteristics, including data processing devices and computers, relating to development and alumni relations.

Advancement Services systems
All systems managed by Advancement Services, including, but not limited to, the CRM database of record, Development and Alumni Relations intranet and Internet sites, online reporting center, online giving and payments, online event registrations and event registrations, e-communications and the alumni website and alumni portal.

Affiliated or institutionally-related foundations
VCU has affiliated philanthropic foundations that are separate 501(c)(3) charitable corporations organized to operate for the support of the university, while operating with self-governed boards and bylaws. They accept and invest gifts made in support of the university.

Authoritative Data Source
The authoritative data source is a recognized and official source for a given data element or a specific piece of information.

Data
Data are sets of signs, signals, facts, or statistics that serve as the fundamental building blocks for information. When collectively placed within context, sets of data can be transformed into information.

Data Stewards
Data stewards are appointed by and accountable to the data trustees. Data stewards must have knowledge of and work in accordance with the policies, standards and guidelines across the institution, including university policies on information security and privacy. Data stewards are expected to be subject matter experts for the business domains under their authority.
Information Asset
Information assets within the context of this document refer to the information that are critical to the operational success of the university, where the loss in quality, security, or availability may significantly hinder the university’s academic, research and administrative missions.

Personally Identifiable Information
- Information that directly identifies an individual (e.g., name, address, or other identifying number or code, telephone number, email address).
- Information about alumni, parents, prospects, donors and other constituents gathered to aid in determining appropriateness of solicitation and level of membership or gift request; specific data in prospect lists that would identify prospects to be solicited; dollar amounts to be requested; and name of solicitor.
- Portions of solicitation letters and proposals that identify the prospect being solicited and the dollar amount requested. Letters, pledge cards, copies of checks or other responses received from or donors about prospective gifts in response to solicitations.
- Portions of receipts, thank you letters or other gift acknowledgment communications that would identify the name of the donor and the specific amount of the gift, pledge or pledge payment.
- Donors’ or prospects’ financial or estate planning information or portions of memoranda, letters, interview notes or other documents about any donor’s or prospect’s financial circumstances.
- Data detailing dates of memberships, gifts, event registrations, payment schedule of gifts, form of gifts or specific gift amounts made by donors.

Vendor
Any company, organization or individual with a contract with VCU or its affiliated foundations for services or other reasons.

Volunteer
Someone who is not employed by Virginia Commonwealth University but works in an official capacity with the university and acts on its behalf.

Contacts
The Office of Development and Alumni Relations (DAR) officially interprets this policy. DAR is responsible for obtaining approval for any revisions as required by the policy Creating and Maintaining Policies and Procedures through the appropriate governance structures. Direct policy questions to the assistant vice president of advancement services within the Office of Development and Alumni Relations.

Policy Specifics and Procedures
Advancement Services oversees DAR Information Technology, Gifts and Records Management, and Prospect Development and Data Management. DAR collects alumni, donor and constituent records required for university business purposes in compliance with legal reporting requirements. DAR strives to maintain the accuracy of the personal data held in its systems and establishes mechanisms allowing alumni to review and correct personal information. All donors must be assured that information about donations are handled with respect and with confidentiality to the extent provided by law. Constituents have regular
opportunities to opt-out of university engagement communications and to request anonymity in their giving records.

**Process for university employees to request data**
Only DAR employees can submit report requests through the DAR Service Desk system. A university colleague should work through their unit’s development contact, or in the absence of a contact, proceed through the ticket system. The DAR employee receiving the data is responsible for maintaining the confidentiality of the data. Information in the reports must not be shared with individuals who do not have explicit approval to see the data.

**Process for VCU volunteers to request data**
Volunteers must sign a DAR Volunteer Confidentiality Agreement, which must be approved by the vice president before any information can be released. All DAR Confidentiality Agreements are kept on file by Advancement Services. Sharing of this data to other volunteers or individuals is prohibited. Report requests that are intended for distribution to volunteers must be clearly identified when the request is submitted. Requests should be made only for the information necessary for a volunteer to perform their university-related role. If the data file is being used for registration check-in or name tags, then all volunteers handling the information must sign the DAR Confidentiality Agreement. Volunteers must not send mass communications by direct mail or email using this list. Volunteers are required to delete or destroy all data after the agreed upon period of time.

**Process for vendors to receive data**
All requests for data to be used with external vendors should be made through the DAR Intranet request form, including requests for direct response vendors, e.g. mailhouses. The university requires the approval of IT Governance, and potentially other procurement offices, prior to any Advancement Services response. The vice president of DAR, or their designee, makes final decisions regarding requests for personally identifiable information, at the recommendation of Strategic Marketing and Engagement and Advancement Services.

**Requests for Advancement Services’ system access**
1. All employees must apply for access to the DAR database of record and to access other Advancement Services systems through the DAR Service Desk. Required training must be completed before access is granted.
2. DAR and university-affiliated foundation staff receive access, upon completion of training and proven knowledge of DAR policies.
3. University unit partners can request access and verification through DAR Talent Management.

**Cancelling system access**
1. If a university employee does not log into the database of record within a 90 day period, DAR may contact the employee to determine a valid reason to extend unnecessary access. Employee access may be cancelled, requiring a new application for login permissions.
2. Unit personnel administrators must notify DAR, through the DAR Service Desk, within 24 hours of staff departure so access can be terminated.
3. Noncompliance with the university’s policies on data management and employee practices will result in immediate cancellation of database access.

**Sharing confidential information with other VCU employees**
DAR employees are responsible for maintaining the confidentiality of data to which they have access. Personally identifiable information must not be shared among divisions. Confidential information received in a VCU email account should not be forwarded to other individuals who do not have a business need for the information. If personally identifiable information needs to be distributed to individuals across divisions, it should be coordinated with Advancement Services to ensure that only authorized individuals have access.

**Forms**

Advancement Services' online request forms are available to university development personnel on the internal DAR intranet.

**Related Documents**

1. [Data and Information Governance](#)
2. [Employee Ethics, Conduct, and Practices Related to University Advancement and Development](#)
3. [Development and Alumni Relations Activities](#)
4. [Computer and Network Resources Use](#)
5. [Information Security](#)
6. [Maintenance and Release of Employment and Personal Information](#)
7. [Payment Card Compliance](#)
8. [Policy on external DAR-related communications](#)
9. [Data Classification Standard](#)
10. [Encryption Security Standard](#)
11. [Information Technology Policies, Standards, Baselines and Guidelines](#)
12. [Personnel Security Standard](#)
13. [VCU Privacy Statement](#)
14. [The Donor Bill of Rights](https://afpglobal.org/donor-bill-rights)
15. [State Government Data Collection and Dissemination Practices Act, § 2.2-3800](#)
16. [State Policy 6.05, Personnel Records Disclosure](#)
17. [State Policy 6.10, Personnel Records Management](#)
18. [Virginia Freedom of Information Act](#)
19. [Virginia Privacy Protection Act](#)

**Revision History**

This policy supersedes the following archived policies:

<table>
<thead>
<tr>
<th>Approval/Revision Date</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>6/29/2019</td>
<td>Minor revisions</td>
</tr>
<tr>
<td>12/2012</td>
<td>This policy supersedes the following BOV policy approved in 5/2009 9.1.1 Advancement Information Technology Data Privacy</td>
</tr>
</tbody>
</table>
FAQ

There are no FAQ associated with this policy