

## Standard Practice Guide Policies

### Use and Release of Donor and Alumni Information

602.05

**Applies to:** All Departments and Units of the University

#### I. POLICY

This policy governs the use and release of all information about development constituents of the University of Michigan. For the purpose of this SPG, “development constituents” will be defined as alumni, donors, prospective donors to the University, and their associated contacts. Information about development constituents that is in the University’s possession is considered institutional data as defined in Standard Practice Guide 601.12 “Institutional Data Resource Management Policy” (<https://spg.umich.edu/policy/601.12>). The University of Michigan owns this information as a University asset and the Vice President for Development in the Office of University Development (“OUD”) is responsible for maintaining it (Regents Bylaw 2.09). This policy is applicable to all campuses and facilities of the University of Michigan.

The policy is intended to allow development personnel, alumni relations’ personnel, and certain others to use information about our development constituents while ensuring that their privacy is protected to the fullest extent permitted by law. The University’s primary source of information about development constituents is the Donor and Alumni Relationship Tool (“DART”). All personnel who want to communicate with development constituents for development and alumni relations purposes must use it, or approved tools which integrate with it.

#### II. DEVELOPMENT CONSTITUENT RELATED INFORMATION

Donor information is defined as the name, any address, telephone number, gift history, ratings or any other information pertaining to a donor or potential donor to the University of Michigan, which is gathered by the Office of University Development (“OUD”), any college, school or unit within the University of Michigan, or any other University employee for development and related purposes.

A. DEFINITION OF ALUMNI INFORMATION. Alumni information is defined as the names, any addresses, telephone numbers or any other information pertaining to alumni of the University of Michigan, which is gathered after the individuals are no longer enrolled as students<sup>1</sup>.

1. GENERAL STATEMENT: Alumni information will not be used or released except as permitted under this policy or as required by law.

2. ACCESS AND USE OF DONOR INFORMATION: Only University employees who have a need to know in order to perform an authorized University function or activity may access alumni information. Alumni information will be used for alumni relations, development and research purposes in accordance with applicable policies.

a. Units may release limited information to volunteers in accordance with OUD’s policy and procedure for Sharing Donor Information with Volunteers Policy and Procedure ([https://docs.google.com/document/d/11QE\\_G45mdA\\_v8BCblYdrBNXhGvyUOYpUHB23a8J1vg/edit](https://docs.google.com/document/d/11QE_G45mdA_v8BCblYdrBNXhGvyUOYpUHB23a8J1vg/edit)).

b. Each unit is responsible for ensuring that its designated volunteers use and distribute the information in the appropriate manner for its authorized function or activity and that the volunteers understand their responsibility to maintain the confidentiality of the information pursuant to these guidelines.

3. RELEASE OF ALUMNI INFORMATION WITHOUT PRIOR PERMISSION OF ALUMNI.

OUD will perform the following functions with respect to requests for alumni information without prior permission of the alumni:

a. Forward Requests. Forward requests from alumni seeking the address of other alumni<sup>2</sup>.

b. Associated Organizations. Alumni information may be released to organizations associated with the University, but not under Regental control, only if the organization certifies in writing that:

(1) It will use the information only in an activity that will directly serve a function of the University. For student-related organizations, the Vice President for Student Affairs or his or her designee must certify that the use of the requested alumni information will serve a University function. OUD will have the final authority to determine if an activity will directly serve a function of the University.

(2) It will not use the information for any other purpose. It will not release or disclose the information to any third party. It will not release the information to a person affiliated with the organization unless that person has a need to know and that person agrees in writing to maintain the confidentiality of the information pursuant to this policy

and other applicable policies and procedures, including Sharing Donor Information with Volunteers.

- e. Alumni Directories and Online Alumni Networking Platforms. OUD may provide alumni information to University of Michigan schools, colleges and units wishing to publish alumni information in a directory or alumni networking platform pursuant to the policy on Alumni Directories and Online Alumni Networking Platforms (SPG 602.06 (<https://spg.umich.edu/policy/602.06>)).

#### 4. RELEASE OF ALUMNI INFORMATION WITH PRIOR PERMISSION OF ALUMNI.

Alumni information may be released in the following circumstances only with the prior written permission of individual alumni. Written permission includes indicators used by online alumni directories and Online Alumni Networking Platforms and updated by the alumni themselves signifying publication is acceptable.

- a. Shared Alumni. When other institutions of higher education request information on alumni who have degrees from the University of Michigan and the requesting educational institution.
- b. Other Alumni. At the request of other alumni.
- c. Recruiting Firms. Requests from management recruiting firms will be forwarded to the appropriate unit placement office for service as authorized by its alumni clients.

#### 5. RELEASE OF ALUMNI INFORMATION UNDER OTHER CIRCUMSTANCES. Alumni information may be released under the following circumstances.

- a. Confirming Degrees. Requests from prospective employers and others should be directed to the Office of the Registrar.
- b. Law Enforcement Agencies. Requests from law enforcement agencies for alumni information should be directed to the Department of Public Safety.
- c. Subpoena Or Court Order. Alumni information will be released pursuant to court order or lawfully issued subpoena. Questions regarding court orders and subpoenas should be directed to the Office of the General Counsel.
- d. All Other Requests. All other requests for alumni information from persons or entities should be directed to the OUD or the Freedom of Information Office, as appropriate.

B. DEFINITION OF DONOR AND DEVELOPMENT PROSPECT INFORMATION. Donor and development prospect information is defined as any name, address, telephone number, gift history, prospect rating(s) or any other information pertaining to a donor or potential donor to the University of Michigan, which is gathered by OUD, any college, school or unit within the University of Michigan, or any other University employee for development and related purposes.

C. ACCESS AND USE OF DONOR AND DEVELOPMENT PROSPECT INFORMATION. Only University employees who are authorized by OUD and who have a need to know in order to perform an authorized University function or activity may access donor information. Donor information shall be used solely for the University of Michigan's development purposes in accordance with applicable policies. . Units may release limited information to volunteers in accordance with OUD's policy and procedure for Sharing Donor Information with Volunteers (<https://policies.dev.umich.edu/sharing-donor-information>).

1. Each unit is responsible for ensuring that its designated volunteers use and distribute the information in the appropriate manner for its authorized function or activity and that the volunteers understand their responsibility to maintain the confidentiality of the information pursuant to these guidelines.

D. REQUESTS FOR DONOR OR DEVELOPMENT PROSPECT INFORMATION. Any requests for donor information by any persons or entities not authorized to receive such information should be directed to OUD or the Freedom of Information Office for handling, except for donors who donate in memory or in honor of someone. The names and addresses of donors who donate in memory or in honor of someone may be released to appropriate family members of that person memorialized or honored.

### III. RESPONSIBILITY FOR IMPLEMENTATION AND COMPLIANCE

In accordance with Standard Practice Guide 601.12 "Institutional Data Resource Management Policy," University Deans and Directors are responsible for implementing this policy and the Vice President for Development is responsible for ensuring compliance with it. These authorities must initiate corrective action with the proper authorities of the University if it is needed. OUD will implement data management practices in accordance with the Data Administration Guidelines for Institutional Data Resources (<https://drive.google.com/file/d/0B7RLnc7LWQbYhPb0x5RmVNOWc/view>).

### IV. MISUSE OF INFORMATION

A. Development constituent information should be used in accordance with Standard Practice Guide 601.07 "Responsible Use of Information Resources" (<https://spg.umich.edu/policy/601.07>). In addition, development constituent information may not be used as follows:

1. To stalk or harass;
2. To solicit for personal purposes or gain, or for institutions not affiliated with the University without proper authorization;
3. To sell, trade, exchange, give, etc. such information to people or institutions not affiliated with the University without proper authorization;
4. To store or transmit donor or alumni information on personally owned devices or via personally maintained services that are not managed by the University without proper authorization;

5. To create any type of database or dataset outside of DART that mirrors or uses DART information but is not integrated with DART without proper authorization. Proper authorization includes approval by the head of the unit and the Vice President for Development.

6. To contact and/or solicit donors, alumni, or parents without following the proper development procedures and permissions.

B. All University employees and affiliates authorized by OUD must access or maintain University-owned sensitive data on personally-owned devices in accordance with SPG 601.33, "Security of Personally Owned Devices that Access or Maintain Sensitive Institutional Data."

C. Disciplinary action may include denial of future access to donor and alumni information, non-reappointment, discharge, dismissal, and-or legal action.

#### V. REFERENCES

Standard Practice Guide 601.07 - "Responsible Use of Information Resources"

Standard Practice Guide 601.12 - "Institutional Data Resource Management Policy"

Standard Practice Guide 601.19 - "Identity Misrepresentation"

Standard Practice Guide 601.25 - "Information Security Incident Reporting Policy"

Standard Practice Guide 601.27 - "Information Security Policy"

Standard Practice Guide 601.33 - "Security of Personally Owned Devices that Access or Maintain Sensitive Institutional Data"

Policy for Sharing Donor Information with Non-Development Professionals - See DevNet or contact "OUD"

<sup>1</sup> Student records are subject to the federal Family Educational Rights and Privacy Act. The Office of the Registrar is responsible for implementing University policy on access to student records.

<sup>2</sup> OUD reserves the right to deny or charge a fee for a voluminous or unreasonable request.

#### File Attachments

Printable PDF of SPG 602.05, Use and Release of Donor and Alumni Information  
(<https://spg.umich.edu/sites/default/files/policies/602x05.pdf>)

<b>SPG Number:</b> 602.05	<b>Applies To:</b> All Departments and Units of the University
<b>Date Issued:</b> July 15, 1991	<b>Owner:</b> Office of the Vice President for Development
<b>Last Updated:</b> February 12, 2021	<b>Primary Contact:</b> Office of the Vice President for Development
<b>Next Review Date:</b> February 12, 2026	

#### Related Policies:

Alumni Directories (/policy/602.06)

Identity Misrepresentation (/policy/601.19)

Information Security (/policy/601.27)

Information Security Incident Reporting (/policy/601.25)

Institutional Data Resource Management Policy (/policy/601.12)

Responsible Use of Information Resources (/policy/601.07)

Security of Personally Owned Devices That Access or Maintain Sensitive Institutional Data (/policy/601.33)