Office of Advancement Oath of Confidentiality

Instructions for Signing and Validation of Identity

Step(s)

a. <u>If you have access to a Printer and Scanner</u>

Please fill in your information on the Digital Form (found below) and print the form then sign in ink, scan the document and attach to a new email.

b. <u>If you do NOT have access to a Printer or Scanner</u>

***** Note that there are Mobile Apps that provide Scanning capabilities, such as the IOs App "Scanner Pro"***

If you are unable to print and/or Scan, please simply type your name in the Signature Box in the place of an ink signature.

Then, send the signed form in an email to dbassist@ucalgary.ca containing the phrase

"I, <Name> have read and understand the Oath of Confidentiality and with my typed signature agree to adhere to the terms and responsibilities set out within the attached document"

University Policy
University Procedure
Instructions/Forms

TERMS AND CONDITIONS OF DATA USE AND OATH OF CONFIDENTIALITY

I, the undersigned, understand that personal information maintained in the University of Calgary's Enterprise Information Systems, not limited to Government contact, donor, prospect, Community partner, donation and alumni related information is highly sensitive and confidential. I acknowledge the importance of controlling and working to minimize the existence of unsecured copies of the University's data to the extent possible and agree to the following Terms and Conditions for use of the data in the Office of Advancement's systems.

Terms and Conditions of Data Use

I further acknowledge that:

a) This data may only be accessed, used, or disclosed for purposes directly related to my work at the University of Calgary;
b) I may only use, enrich, alter, change, modify, or delete existing personal information in accordance with applicable legislation and policy and if I am authorized to do so;
c) Information, regardless of format, extracted from Enterprise Information Systems may only be shared if absolutely necessary with individuals with a current signature to the Terms and Conditions of Data Use and Oath of Confidentiality (Can be confirmed by contacting Advancement Data);
d) Access to, use and disclosure of this information is governed by the Freedom of Information and Protection of Privacy Act of Alberta and these University policies (see last page); and,
e) Data extracted from Enterprise Information Systems will be stored in a secure environment with reasonable protection against risks of unauthorized access, collection, use, disclosure or destruction.

I also acknowledge that confidential information provided to the user by Advancement Data:

f) Is without exception authorized for single-use, only for the purpose and in the manner described and agreed upon by the user and the information provider in the original ServiceNow Request;
g) Will be used only by the user(s) authorized for the single use specified and will be promptly permanently deleted immediately after its use;
h) Will not be repurposed, copied nor stored for any reason beyond its predefined expiry date (see point [i] below);
i) Must be destroyed (or returned to data steward if appropriate) within 30 days after receipt ("expiry date"), or alternate date agreed to in advance, in which case, the acceptable use duration will be documented in the Request Item in ServiceNow.

In Case of Data Breach

In the event that the user becomes aware of a breach of security relating to the information provided by any unit within Advancement under the terms of this agreement, the proponent will notify the Data Steward by emailing alyson.kenward1@ucalgary.ca immediately with details as follows:

a) The nature of the information that was breached
b) When and how the breach occurred, if known

c) Who was responsible for the breach if known
d) What steps if any have been taken to mitigate the matter
e) What measures have been taken to prevent recurrence.

The data recipient/user will not assign this agreement or any rights hereunder to another person or entity without the prior written consent of the Data Steward. This includes assignment to volunteers or external partners/affiliates.

In keeping with the Electronic Communications Policy, the Advancement Data team will be permitted to audit data usage, if required, to ensure compliance with the terms & conditions of this agreement.

Questions or concerns regarding the terms and conditions for sharing, using or distributing the Office of Advancement's data assets shall be directed to:

Scott Zimmer (Data Custodian)
Director, Advancement Data

Office of Advancement
University of Calgary
Olympic Volunteer Centre (OVC)
scott.zimmer@ucalgary.ca

Office: (403) 210-7657

The recipient/user is ultimately responsible for the appropriate usage of the data. Violations of these terms & conditions will result in disciplinary action based on the severity of the violation up to and including termination of employment or volunteer position. This agreement remains in force for as long as the user has access to Advancement's data assets and systems. Access to systems and data requires annual renewal of this agreement through physical or digital signature as the situation warrants.

Select a Category: □ Staff □ Faculty □ Volunteer □ Contractor/Affiliate

Executed by:
Name (print): _____ UCID _____

Title & Team: _____

Signature: _____

Date: _____

By signing the Terms and Conditions of the Oath of Confidentiality, you agree to the terms and conditions outlined in UCalgary policies. These terms and conditions include but are not limited to:

Policy	Key Responsibilities / Obligations / Commitments (referenced sections noted below)
Acceptable Use of Personal Information in Enterprise Information Systems Policy	4.4 Individuals who are granted access to an Enterprise Information System must abide by all applicable restrictions, whether or not those restrictions are built into the operating system or network and whether or not they can be circumvented by technical means. 4.5 Individuals will access or use Personal Information in an Enterprise Information System only if it is necessary for a work related purpose. 4.6 Individuals who have access to an Enterprise Information System will not disclose Personal Information obtained from the system to anyone other than persons who are authorized to receive the information, that is, persons who need the information for a work related purpose.
Acceptable Use of Information Assets Policy	4.3 At a minimum, users are responsible and will be held accountable for: a) knowing and complying with University policies, procedures and standards relating to the use of Information Assets and systems; b) safeguarding the Integrity and Confidentiality of University information as outlined in this and other University policies; and c) creating, accessing, using and disposing of University information based on its classification.
Electronic Communications Policy	4.15 Electronic communication is an inherently insecure means of communication. An Authorized User will ensure that the contents of a message are secured in accordance with the Information Security Classification Standard when using e-mail and other electronic technology to distribute Confidential Information to an external address. 4.22 Authorized Users should be aware that the recipient of their message may forward the message to others without recognizing the need to seek their consent. Authorized Users shall clearly identify those messages that are considered confidential and which should not be forwarded without permission.
Information Security Classification Standard	Appendix 1: Personally Identifiable Information (PII) is Level 3 (Confidential) which entails limits to who can Read / Write / Edit / Access. Encryption (or similar mechanism) is required when transmitting via public or local networks.
Privacy Policy	4.7 Personal Information will not be used for a purpose other than the purpose for which it was collected or for a use consistent with that purpose except with the Consent of the individual or as permitted under FOIP. 4.12 The University will take reasonable steps to ensure that Personal Information in its custody or under its control is as accurate and complete as is necessary for the purposes for which it is to be used. 4.17 The University will retain Personal Information only as long as necessary for the fulfillment of its purposes as defined in its retention rules. 4.18 The University will take reasonable steps to protect information from unauthorized access, collection, use, disclosure or destruction.