SNAAP PARTICIPATION AGREEMENT – 2022 SNAAP SURVEY

---

1) Purpose of SNAAP Survey

a) The Strategic National Arts Alumni Project Participation Agreement ("Agreement") is entered into between Arts + Design Alumni Research, Inc, also known as the Strategic National Arts Alumni Project or SNAAP ("SNAAP") and[ ] ("Participating Institution").

b) The SNAAP survey is an online survey, data management, and institutional improvement system designed to enhance the impact of arts-school education. SNAAP provides national data on how artists develop, helps identify the factors needed to better connect arts training to artistic careers, and allows education institutions, researchers, and arts leaders to look at the systemic factors that help or hinder the career paths of arts-school alumni. The SNAAP survey is conducted by SNAAP in partnership with The University of Texas at Austin, College of Fine Arts and The University of Illinois at Urbana-Champaign, College of Fine + Applied Arts.

c) SNAAP Survey administration protocol is approved by The University of Texas at Austin Institutional Review Board (IRB)

2) SNAAP Data Management Procedures and Safeguards

a) SNAAP takes individual privacy seriously. SNAAP is committed to implement, maintain, and use appropriate administrative, technical, and physical security measures to preserve the confidentiality and integrity of protected private information.

b) SNAAP survey participant data is encrypted in transit and at rest. SNAAP uses 2048-bit public key encryption with a 128–bit SSL connection to ensure the security of survey and other sensitive data that are transmitted across the Internet. The security procedures used by the SNAAP are equal to or surpass the requirements for transmitting confidential information. Access by SNAAP staff to servers storing institutional data is controlled by user IDs and passwords. SNAAP strictly limits access to protected SNAAP data its own employees, contractors, and those individuals who are authorized by SNAAP for the proper handling of such information.

c) SNAAP contracts with Indiana University's Center for Survey Research (CSR) to provide security for SNAAP software, data, and survey administration. The servers storing SNAAP institutional data are managed by CSR. The CSR computing environment has robust physical, electronic, and procedural security system safeguards, the details of which are listed below:

(1) The computing environment at the CSR requires and maintains a high level of computer and data security per the ***policies governing IU information technology resources*** ***and***

data. *The University Information Technology Services Policy Office (UIPO) at IU provides a baseline level of enforced security requirements including protocols to prevent unauthorized access to IU computers. The CSR computing staff uses industry standard best practices as our security procedures. Each CSR workstation is updated daily with virus protection software. CSR endpoints are scanned daily for needed security patches and hot-fixes. The centralized security server deploys all needed Microsoft security patches each night and machines are audited weekly to verify security patches are up to date.*

(2) *The CSR employs the Principle of Least Privilege when assigning access rights to staff. The systems administration staff has designed a number of processes for preventing intrusions or data loss on the CSR's servers. Remote access to the servers is tightly controlled by userIDs, passwords, and two-factor authentication through DUO. Physical access to servers is restricted per the security protocols of* ***IU's data center****. Access to directories on the file servers is restricted to only those employees who need access. Security processes similar to those run on the workstations are used to prevent, detect, and repair security problems on the servers. The servers are located on a range of private IP addresses restricting their access from the outside world. The servers sit behind a network firewall, and employ their own machine firewall. IU provides security scanning of our servers to look for possible problems and the computing staff carefully monitors server event logs for possible attempts at intrusion.*

(3) *Individual workstations are part of a Virtual Lan (VLAN) which allows even greater restriction of access. Any remote access requires remote authorization and a connection using an SSL VPN behind two-factor authentication.*

(4) *The files on the servers are backed up each night, and all project data is encrypted at-rest within the backup. The file and web servers are virtual systems employing RAID 5 technology to ensure that a disk failure will not cause any loss of data. They are located in a modern class 4 data center designed to meet FEMA standards for surviving an F5 tornado among other natural disasters. The building is staffed 24x7 and employs all modern physical security measures.*

(5) *The CSR uses 2048-bit public key encryption with a 128–bit SSL connection to ensure the security of survey and other sensitive data that are transmitted across the Internet. The digital certificates were issued by InCommon/COMODO and are used by the survey respondent's browser to verify that the user is connected to the website that matches the name in the URL. The browser and the server then encrypt and exchange keys that are used to encrypt the remainder of the session. Through the use of these keys, the data are transmitted using the SSL. The security procedures used by the CSR are equal to or surpass the requirements for transmitting confidential information.*

d) Institutionally identifiable SNAAP results shall not be made public by SNAAP except by mutual agreement between SNAAP and Participating Institution, or when required to do so by law. Except as otherwise prohibited by law, SNAAP will promptly notify the university of any subpoenas or other legal orders received by SNAAP seeking university supplied data and consult with the university regarding the information that will be disclosed. SNAAP will cooperate with

reasonable requests in connection with efforts by the university to intervene and quash or modify the subpoena or other legal order.

e) SNAAP will partner with AlumniSync (or a similar alumni tracking company) to provide new and updated contact information for Participating Institutions alumni. Any new and updated contact information will be provided to Participating Institution following the administration of the survey. Participating Institutions can opt out of this free service; if the institution chooses not to utilize this service, the institution must notify SNAAP directly at a date to be determined.

f) SNAAP project staff may use de-identified survey data in the aggregate for national reporting purposes.

g) SNAAP may make de-identified data in which individual respondents or institutions cannot be identified available to interested and qualified researchers on a limited and basis as a source of data for researchers. SNAAP will strip all respondent and institutional identifiers from any data set that will be shared externally. No open-ended responses will be shared externally. SNAAP may include institution-level information (e.g., Carnegie Classification) but not in a way that individual schools can be identified directly or indirectly. Researchers will be required to comply with standard industry data security requirements and will be prohibited from sharing the data any further. SNAAP may ask researchers to pay a fair cost recovery price for the time and effort put into collecting and managing the data, and for preparing the data for use by researchers.

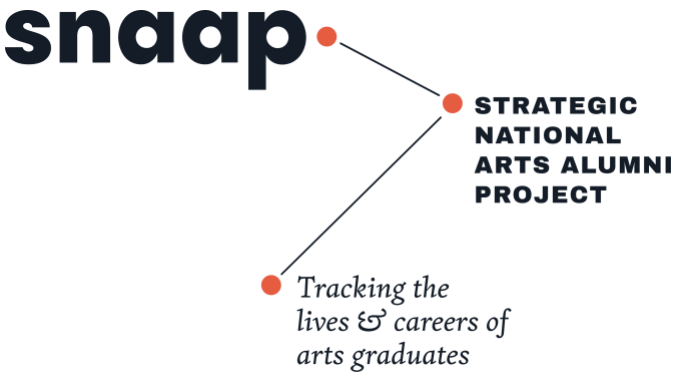
h) Participating Institution will be charged based on the number of arts degrees conferred by Participating Institution in 2019/20 (verifiable by IPEDS data), as reported to the U.S. Department of Education.

i) **Participating Institution Procedures and Requirements**

(1) Participating Institution agrees to provide an alumni population data file containing contact information as defined by SNAAP population file guide-lines. SNAAP will not use population file data for any purpose other than the SNAAP survey. SNAAP will not release contact information to a third party unless Participating Institution gives the express authority to do so (as in the case of AlumniSync or other alumni search firm) or unless required to do so by law.

(2) Participating Institution will customize its survey administration on the secure online SNAAP interface. The Participating Institution's response rates, Institutional Reports and complete dataset (when available), and other information will be housed on the secure SNAAP interface and accessible to all Participating Institution authorized contacts.

(3) Participating Institution is encouraged to send general promotional announcements to its alumni about the survey, but will be asked not to contact individual alumni directly to recruit them for the project without prior approval from The University of Texas at Austin



IRB. Participating Institution must present the SNAAP Survey as a voluntary activity; no coercion can be used to increase participation.

(4) Participating Institution must seek SNAAP's approval of any alumni participation incentives (e.g., lottery drawings and prizes) to ensure compliance with IRB requirements.

(5) Participating Institution shall pay SNAAP all applicable fees related to the survey within thirty (30) days of receipt of the survey invoice, unless alternate payment arrangements are requested.

j) **Use of Alumni Data and FERPA Compliance**

(1) Under this Agreement, Participating institutions will provide SNAAP with the following personally identifiable data elements: first and last name, gender, mailing address, phone number, email address, degree pursued, major, level of degree pursued, cohort or graduation year, department/school/college information, and other information chosen by Participating Institution.

(2) FERPA Compliance. Personally identifiable student education records provided to SNAAP in the course of providing services under the Agreement are subject to the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. 1232g, et seq. and the regulations promulgated thereunder. Such information is considered confidential and is therefore protected ("educational records"). To the extent that SNAAP has access to "education records" under this Agreement, SNAAP is deemed a "school official," as each of these terms are defined under FERPA. SNAAP agrees that it shall not use education records for any purpose other than in the performance of this agreement. Except as required by law, SNAAP shall not disclose or share education records with any third party unless permitted by the terms of the contract or to subcontractors who have agreed to maintain the confidentiality of the education records to the same extent required of SNAAP under this agreement.

(3) Educational records supplied by University to SNAAP are the property of university and shall not be sold or used by SNAAP, internally or externally, for any purpose not directly related to the scope of work outlined in a this SNAAP Participation Agreement between the Parties without the written permission of university. Upon termination of the Agreement, SNAAP will return and/or destroy all personally identifiable student educational records data or information received from the University upon, and in accordance with, direction from university.

(4) SNAAP agrees that in the event of any breach or compromise of the security, confidentiality or integrity of any university provided data where personally identifiable information of a University student, prospective student, employee, alumnus or other University affiliated person was, or is reasonably believed to have been, acquired and/or accessed by an unauthorized person and where such breach is known to SNAAP or upon notification of such breach to SNAAP, SNAAP will promptly notify University of such breach or compromise, cooperate with all notification actions and assist University with

all reasonable notification actions required by University policy and applicable law.

(5) With respect to its use and handling of personally identifiable data received from the Participating Institution, SNAAP will:

(a) Ensure the alumni survey responses provided to Participating Institutions are stripped of all identifiers so that alumni responses are anonymous to institutions. Note: The SNAAP survey may provide an alumni participant with an opportunity to voluntarily provide a narrative or open ended response and comment on the SNAAP survey, which may, at their discretion, include information that can be classified as, or associated with, Personal Information. Although SNAAP will never identify a participant to their affiliated institution by name, SNAAP will disclose the text of their response or comment to their affiliated institution in the context of that response or comment, and by their submitting such a voluntary narrative or open ended response or comment on the SNAAP survey, they affirmatively consent to its disclosure to their affiliated institution without any added expectation of confidentiality in connection with it.

(b) Use such data only for the purposes of conducting studies designed to improve arts training, inform cultural policy, and/or support artists as well as studies that evaluate the effectiveness of SNAAP survey methods in order to improve future data collection.

(c) Only use alumni contact data for the purposes of inviting alumni toparticipate in the SNAAP survey, or to evaluate the effectiveness ofsurvey administration methods;

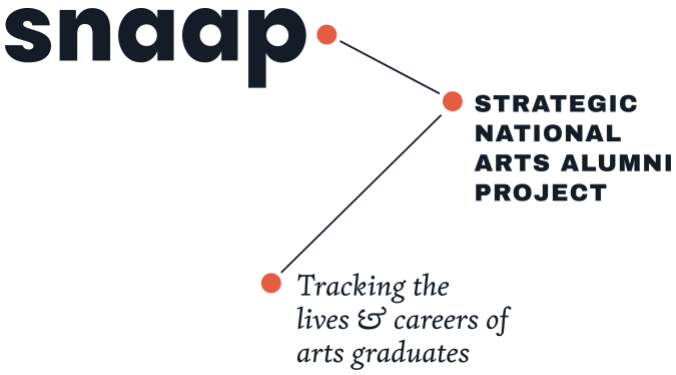
(d) Use Secure Sockets Layer (SSL) software to encrypt information during transfer from Participating Institution to SNAAP;

(e) Limit access to such data to representatives of SNAAP who have legitimate interests in the information for the purposes described above;

(f) Not provide Participating Institution's data to a third party except aspermitted in this Agreement;

(g) Use the data in the aggregate for national and sector reporting purposes;

(6) Unless a Participating Institution opts out prior to providing its data files to SNAAP, SNAAP may partner with AlumniSync or a similar alumni tracking company to update and correct alumni contact information provided by the Participating Institution. SNAAP will provide Participating Institution with the updated and corrected alumni contact information following the administration of the SNAAP survey to Participating Institution's alumni.



(7) SNAAP may retain Participating Institution de-identified data in its database. The parties understand and agree that SNAAP will maintain de-identified SNAAP survey response data for an indefinite period of time, in order to enable longitudinal study of arts career trends and other analyses.

3) Assignment. This Agreement shall not be assignable by either party without the prior written consent of the other party.

4) Force Majeure. Neither party shall be responsible or liable to the other party for nonperformance or delay in performance of any terms or conditions of this Agreement due to acts of God, acts of governments, wars, riots, fire, flood, or other causes beyond the reasonable control of the nonperforming or delayed party.

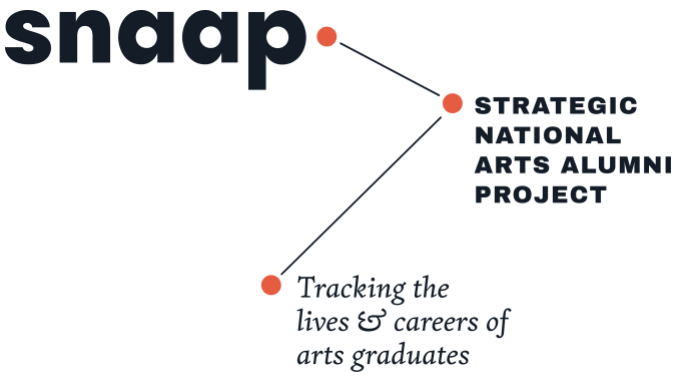
5) Limitation on Liability. Participating Institution agrees that SNAAP, The University of Texas at Austin, and its trustees, affiliates, employees, agents, and contractors, shall not be liable to Participating Institution for any claims, liabilities, consequential or incidental damages, costs, or expenses relating to this Agreement for an aggregate amount exceeding the fees paid by Participating Institution to SNAAP.

6) Compliance with Data Privacy and Transfer Laws. SNAAP will comply with applicable data protection laws and regulations protecting the privacy of persons. SNAAP will not collect, store, process or transmit cardholder or sensitive authentication data, as defined by the Payment Card Industry Data Security Standard. SNAAP will not collect, store, process, or transmit financial services data as defined by the Gramm-Leach-Bliley Act. SNAAP will not transfer personally identifiable information in violation of data protection laws and regulations protecting the privacy of persons as defined by EU General Data Protection Regulation ("GDPR"). All transfers under this agreement will be necessary for the performance of agreements between the data subject and either or both parties, requiring no GDPR Model Clauses or Standard Contractual Clauses in accordance with EU Decisions, Directives and Regulations. In the event of any transfers across country boarders, the Participating Institution and SNAAP will not be the entities that are transferring the data across country borders – rather, the data subjects themselves will be voluntarily doing the transferring. Neither party will be expected or obliged to transfer any personal data to the other party in breach of applicable data protection laws.

7) Independent Contractor. The relationship between SNAAP and the Participating Institution under this Agreement will be that of independent contractors. Neither party is an agent, joint venture, partner, or employee of the other party

8) Severability. Should any provision of this Agreement be found to be invalid, illegal, or unenforceable for any reason, the invalidity or unenforceability of such provision shall not affect the validity of the remaining provisions hereof, unless such invalidity or unenforceability would defeat the purpose of this Agreement, in which case, either party may terminate this Agreement by giving written notice.

9) Notice. Any notice, consent or other communication required or contemplated by this Agreement shall be in writing, and shall be delivered in person, by U.S. mail, by overnight courier, or by



electronic mail to the intended recipient at the address provided in this Agreement. Notice shall be effective upon the date of receipt by the intended recipient.

10) Termination. Either party may terminate this Agreement upon thirty days (30) days prior written notice to the other. In the event that either party hereto shall commit any material breach of or default in any terms or conditions of this Agreement and also shall fail to reasonably remedy such default or breach within fifteen (15) days after receipt of written notice thereof, the non-breaching party may, at its option and in addition to any other remedies which it may have at law or in equity, terminate this Agreement by sending notice of termination in writing to the other party to such effect. Termination shall be effective as of the day of the receipt of such notice. Termination of this Agreement by either party for any reason shall not affect the rights and obligations of the parties accrued prior to the effective date of termination of this Agreement.

11) Entire Agreement. This Agreement constitutes the entire agreement between the parties regarding the subject matter described herein and supersedes any prior negotiations and agreements. This Agreement may not be modified or amended in any respect except by a written agreement executed by both parties. The terms and conditions of this Agreement shall extend to, be binding upon, and inure to the benefit of the heirs, administrators, representatives, executors, successors and assigns of the parties.

IN WITNESS THEREOF, the parties hereto have executed this Agreement as of the Effective Date.

By:	By:
Date:	Date:
Lee Ann Scotto Adams, *Executive Director, SNAAP*	[Name] [Title]