Student Data Release Policy and Guidelines, Brown University

Last modified August 3, 2018

The University policy on the release of student data is outlined in the following set of guidelines. Student data included in this policy refers to information collected about the student by the University as part of its normal business operations. Various offices at the institution receive requests for student data from within and outside of the Brown community. In some cases, data requested are already protected from disclosure by preexisting laws (e.g., for students, the Family Educational Right to Privacy Act, or FERPA) or institutional policies around the confidentiality of information.

This document is designed to provide guidance in submitting and responding to requests for student data. There may be cases when data usage agreements will need to be completed prior to disclosure of the data.

The process is distinct from the Institutional Review Board (IRB) review and approval process for protection of human subjects. IRB approval does not guarantee approval under these guidelines.

I. Data Release of Individual Student Data

- Brown's FERPA Policy permits the release of student "directory information" at the discretion of the University without the prior consent of the student (with the exception of students who have specifically restricted the release of this information). Brown University does not provide directory information requested in list or bulk form, including student emails, except when required by law or where specifically approved by the Provost or President. Such approval is generally limited to national or consortial research programs with which the institution has a prior relationship, or governmental research programs in which the University is legally bound to participate. Even in these cases, relevant FERPA and IRB guidelines will be followed.

- Student data, beyond directory information, can be released internally to faculty and staff with a "legitimate educational interest." A faculty or staff member has a legitimate educational interest if the faculty or staff member needs to review student data in order to fulfill a professional responsibility. Examples of this could include advisors; academic department chairs; and deans or senior officers responsible for planning and evaluation. Persons receiving such information are prohibited from releasing it to anyone else, whether internal or external to the institution. Student data, including email lists, will not be provided to faculty or students for course work or course-related projects.

- In rare cases the President or Provost may request release of data on individuals for projects of extreme institutional and/or national importance where Brown is assured of the confidentiality of the data and where such release is permitted by FERPA. The Data Governance Committee will review these requests and consult with the Office of the General Counsel as necessary. Restricted data elements

such as confidential health information; social security numbers; bank account numbers; and other private information will not be considered for release. See Brown policy on risk classifications. As part of the deliberation, considerations of privacy, transparency, obligations under applicable law and University policy, and institutional resources will be considered in addition to the direct benefit of the research to the planning, programming, and educational offerings of Brown University. Release of individual student data will also be considered when active informed consent that explicitly lists data elements to be released has been given by the student. Student consent does not guarantee release of all data elements.

II. Data Release of Aggregated Student Data

- Information on groups (aggregate data) is released if it is already published: i.e., if it is in the public domain. For example, data published on enrolled and degrees completions on the National Center for Education Statistics web site; and information on degrees; enrollment; survey results; alumni outcomes etc. routinely published on the fact book website of the Office of Institutional Research.

- Such data will normally be made available only in the same form in which they have been published. Requests for data in a re-aggregated format, or in any other kind of different form, can be honored only if allowed by applicable law and if resources permit.

- Information on groups is not released in some cases. For example:
    - When it might be possible to infer individual information from it, i.e., if the number within a particular subset of the aggregation were small and its personal attributes sufficiently distinctive.
    - It is considered to be private information on the aggregate as well as the individual level, e.g. grade distribution by department or student subset.
- In cases of requests that do not fall clearly into either the permitted or non-permitted release category, the data trustees of the relevant area will make a decision consistent with applicable law and University policy on a case-by-case basis. Senior officers of Brown University or the Data Governance Committee will be consulted if needed.

- Provided that a student's privacy is protected and the request is consistent with applicable law and University policy, decisions to release aggregate data will be based largely on the benefit to Brown weighed against the resources that must be allocated to producing the data and the availability of such resources at that point in time. Such requests should normally be submitted in writing.

- When a determination has been made by the appropriate data trustee or under an existing policy that individual information can be made available, it will be released to those persons internal to Brown University who are institutionally

responsible for the category of students, faculty, or staff of which the individual is a member. For example, an academic department chair may have access to information on their concentrators but not concentrators of other departments.

- Administrative individual level data on multiple groups can be provided to administrative offices (e.g. Office of Institutional Research; Data Science) supporting the planning and evaluation of the University.

III. Access to Student Data for Faculty and Students

- Student data will not be provided to students for use in student coursework, student research, or special projects.
- Student data will not be provided to faculty for research except in rare exceptions as noted in the rare release of data described in **Section I**, **Data Release of Individual Student Data**
- Faculty and faculty committees seeking to use student data for internal planning and evaluation must have University sponsorship by the relevant senior officer. The data request must be submitted to Office of Institutional Research by the administrative sponsor and must include information on the intended use and audience. This data cannot be distributed beyond its original intent and the project leader is responsible for the security of the data and for ensuring that the data is only disclosed to those authorized by the senior officer.

IV. Responsible Use of Student Data

- Student data provided on the areas of the University's websites that are accessible to the general public are considered public information and can be used freely.
- Student data provided on areas of websites that require individuals to submit their authentication credentials is intended for the sole use and benefit of members of the Brown community, are considered restricted and non-public information, and the University discourages the sharing of restricted and non-public information beyond the Brown community.
- Any data that has been provided to members of the Brown community as part of an official data request shall be used only for the purposes outlined in that request.
- Members of the Brown community who receive student data are responsible for informing the appropriate senior officer and the Office of Institutional Research in the event of a data breach, if these data are lost or stolen, or if the data has been copied or stored on a computer or another electronic device that is lost or stolen.
- Individuals or groups of students, faculty, and staff who share restricted and non-public information beyond the original stated purpose and without express written consent from the senior officer or Office of Institutional Research may be subject to disciplinary action.