



DISTRICT OF COLUMBIA

OFFICE OF THE STATE SUPERINTENDENT OF

EDUCATION

YRBS DATA REQUEST AND PROTECTION PROCEDURE

Last updated April 2, 2019

District of Columbia Youth Risk Behavior Survey (YRBS) data are made available only under a special data sharing agreement (known as a Memorandum of Agreement, or MOA) with the Office of the State Superintendent of Education (OSSE). OSSE has promised anonymity to all YRBS student respondents and protection of their data to the fullest extent available by federal and state law. OSSE takes this promise seriously, and it is the basis for this process.

YRBS data are highly sensitive. The combination of census administration, small geographic areas and small student subgroups increases the risk of unmasking of student identity, even absent student names. As a result, OSSE has adopted a policy and procedure for disclosure of YRBS data and imposes rigorous restrictions on YRBS data sharing to enhance the protection of student privacy.

The remainder of this document outlines the materials to submit to apply to receive YRBS data from OSSE. If approval is granted, OSSE will send an MOA to the applicant for institutional review and signature. Our experience is that the process from MOA negotiation to data fulfillment can take months. Requestors should plan accordingly.

Please complete the online data request form (<https://osse.dc.gov/service/osse-data-request-form>) and submit additional application materials (detailed below) electronically to: OSSE.Datasharing@dc.gov.

Research Plan

All applicants for YRBS data must provide a short (one- to three-page) research proposal that includes a statement of the goals of the research and specifies:

- The variables from the YRBS dataset you intend to use in your research.
- What other data, if any, you plan to merge with the YRBS data.
- Why you believe other available data sources, if any, are not adequate for your research purposes.
Why the research will benefit DC students and align with [OSSE's strategic goals](#).

Curriculum Vitae Requirement (for Academic Requesters)

Applicants for YRBS data from academic institutions must provide Curriculum Vitae (CVs) for all who request YRBS data access. Please ensure that you and your staff meet

the requirements for obtaining the data. All studies must be conducted or supervised by a Primary Investigator (PI). The PI must be an individual who has a permanent, full-time, doctoral-level appointment, typically at an academic institution. Other academic institution personnel or graduate students who wish to obtain the YRBS dataset for purposes of conducting educational research must be sponsored by a permanent, full-time doctoral-level faculty member who takes all responsibility for the protection of the data and is the primary signer on the agreement. Submit a copy of the academic resume or curriculum vitae for the PI, as well as those of all participating research staff.

Data Protection Plan

All applicants must submit a Data Protection Plan that describes the following elements of the work and computing environments.

1. Types of Protection Expected

The following data protection requirements apply for YRBS data. Your data protection plan should describe how your work environment will protect the data, for each of these features or their equivalent:

- Data may be used only by individuals with authorization in the agreement for data use.
- Data use must be in office environment described in security plan and not at home or any other off-site location.
- All computers storing data are password-protected.
- All computers storing data feature an automatic activation of password-protection after five minutes of inactivity on the computer.
- No automated backup copying of the data, including to institutional servers.
- Any and all removable devices holding the data (e.g., CDs, diskettes, zip drive disks, etc.) are stored through encryption and storage in a locked compartment or room when not in use.
- Detailed printouts derived from data analysis are stored in a locked compartment or room when not in use.
- All detailed listings and printouts that are no longer needed are shredded.
- Pledge to destroy all files containing YRBS at the end of the project in accordance with OSSE's Shared Data Destruction Policy (https://osse.dc.gov/sites/default/files/dc/sites/osse/service_content/attachments/OSSE%20Data%20Destruction%20Policy.pdf) and the agreement's requirements.
- Report any and all violations of the Data Protection Plan to OSSE, the Primary Investigator and the home-institution IRB within **24 hours** of awareness of the violation.
- No transmittal of data or detailed tabulations with cell sizes of fewer than **10** in the numerator and **30** in the denominator via e-mail or e-mail attachment or any

other method (such as over the Internet, an Intranet system, or within a local area network).

- Brief all research staff with access to the YRBS data about the Data Protection Plan, appropriate data use, and penalties for inappropriate use.
- The PI must regularly monitor procedures for use of the data by all project staff and collaborators. Clear rules about YRBS data use should be posted in a location that is readily visible to staff. At the conclusion of the research project, all the original YRBS media must be destroyed and all data files and unpublished printouts must be destroyed in compliance with OSSE's Shared Data Destruction Policy and the MOA's requirements.

2. Disclosure Avoidance Rules

The Data Protection Plan must describe how researchers and their staff will avoid inadvertent disclosure of respondents' geographic locations or identity in all working papers, publications, and presentations. At minimum, researchers must agree to exclude from any type of publication or presentation, the following information:

- Listing of individual cases.
- Description of individual cases.
- Listing, description, or identification of a tract or tracts by number, by name, or by descriptive information.
- Listing by school or Ward of school.
- Summary statistics or tabulations with cell sizes of fewer than 10 in the numerator and 30 in the denominator.

3. Data Protection Plan Description

The data protection plan must:

- List and describe all locations where the original and any copies of the data will be kept (and provide building name, street address, and room numbers);
- List names (and, for academic institutions, include CVs) of all individuals who will be accessing the data;
- Describe the computing environment in which the data will be used, including:
 - Computing platform (e.g., personal computer, workstation, mainframe) and operating system;
 - Number of computers on which data will be stored or analyzed;
 - Physical environment and address in which computer and data are kept (e.g., in room with public access, in room locked when not in use by research staff);
 - A list and description of all devices on which data will be stored (e.g., mainframe computer storage device, PC hard drive, removable storage device such as CD, floppy drive, or zip drive);

- Methods of data storage when data are not being used;
- Methods of transmitting the data and results between research team members (if applicable);
- Methods of storage of computer output both in electronic form and in hard copy (on paper or other media); and
- Instruction in data protection policies that will be provided to each staff member and student before they receive access to the data as well as recurrent instruction that will be conducted at least annually.

4. Human Subjects Review and Certification

Human Subjects Review. You must provide evidence of review by your institution's Institutional Review Board/Human Subjects Review Committee/Privacy Board. No exempt or abbreviated review, or lower standards, such as are sometimes used for "secondary data analysis," may be used in this aspect of the human subjects review. A letter of approval or other documentation should be submitted electronically along with the certification document (below).

Certification. The Chair of your institution's Institutional Review Board/Human Subjects Review Committee/Privacy Board must certify that the Board/Committee has reviewed and approved your Data Protection Plan (and the portions of your Research Plan that deal with respondent anonymity and data security, if any), as approved by OSSE, in accordance with the standards and procedures used for live human subjects. The attached memo, "Certification of Human Subjects Review," should be used for the certification.

5. Memorandum of Agreement (MOA) for YRBS Data

Upon approval of the application materials by OSSE, an e-version of OSSE's YRBS agreement will be sent for institutional review and signature. The Investigator(s), or signatory authority at a DC Government agency, must sign it. The Investigator(s) or DC Government agency point of contact, then send(s) the signed agreement back to OSSE, where the State Superintendent will sign it.

Note: In the event that the PI changes institutions, the agreement is no longer valid and a new one must be completed and it must include a revised data protection plan reflecting the new work environment and Human Subjects Review by the investigator's new institution. All original data and any derived analysis files must be destroyed in compliance with OSSE's Shared Data Destruction Policy until the new agreement is established, signed and fully executed.

Memorandum to Institutional Review Boards/Human Subjects Review Committees

TO: Institutional Review Boards/Human Subjects Review Committees

FR: Gwen Rubinstein, Manager, Data Governance and Policy, Division of Data, Assessment and Research, OSSE

RE: Review of Proposals for Analysis of Youth Risk Behavior Survey Datasets

The Youth Risk Behavior Survey (YRBS) is a biennial survey of important health-related risk and protective factors and is sponsored by the Centers for Disease Control and Prevention (CDC). The Office of the State Superintendent of Education (OSSE) makes YRBS data available only to researchers who meet rigorous conditions. The District of Columbia's YRBS datasets are census-level and contain information that OSSE believes increases the potential risk of re-identification of study participants.

It is because of the potential risk of re-identification of participants that OSSE requests that you review portions of proposals to use District of Columbia YRBS data, and to do so using the same standards you would use for surveys of live human subjects. Although researchers using the YRBS datasets are conducting "secondary data analysis," the increased potential risk of re-identification of YRBS study participants makes inappropriate the usual "exemption" applied to "secondary analysis" of anonymized datasets.

We request that you review specifically the Data Protection Plan, and those aspects of the Research Plan that deal with issues of respondent anonymity and data security, if any. We ask for your review because you will be better able to judge the extent to which, in your institution's physical and computing environment, the Plans are adequate to ensure participant anonymity and limitation of access to the restricted data to the persons specified in the agreement.

We are **not** asking that you review the entire YRBS. That review has been done by the relevant committees at the CDC and the primary sponsors of the YRBS.

For questions about the nature and scope of these requirements, contact:

Gwen Rubinstein
Division of Data, Assessment and Research
Office of the State Superintendent of Education
1050 First Street NE, 4th floor
Washington, DC 20002
(202) 899-6132
Gwen.Rubinstein@dc.gov

Certification of Human Subjects Review

Restricted Data Investigator:

Title of Research Proposal:

As Chair of the Institutional Review Board/Human Subjects Review Committee of the Institution specified below, I certify that:

1. Our Institutional Review Board/Human Subjects Review Committee meets requirements established by the Department of Health and Human Services for Multiple Project Assurances or Federal-Wide Assurances;
2. Our Institutional Review Board/Human Subjects Review Committee has reviewed, according to its standards and procedures for live human subjects, and approved, the Data Protection Plan (and those portions of the Research Plan that deal with respondent anonymity and data security, if any), approved by OSSE of the Research Investigator above; and has approved those plans.

Signature Date

Typed name

Title

Institution

Building address

Street address

City State ZIP Code

Phone

Email address