# Plan Overview

A Data Management Plan created using DMPonline

Title: London Sexual Violence Project

Creator:Suzanne Hamilton

Principal Investigator: Neil Humphrey

Data Manager: Suzanne Hamilton

Contributor: Claire Fox, Ola Demkowicz, Jo Deakin, Carla Mason, Lesley-Anne Carter

Affiliation: University of Manchester

Template: University of Manchester Generic Template

ORCID iD: 0000-0002-8148-9500

Project abstract:

Dating and relationship violence (DRV), including psychological, physical, sexual and technology-facilitated abuse, is a significant public health concern associated with adverse mental health, educational and social outcomes. DRV is common among adolescents in England and Wales and disproportionately affects some groups, including girls, sexual and gender minority young people, and those with special educational needs and disabilities. Early intervention is therefore critical to address harmful attitudes before patterns of violence become established. The London Sexual Violence Programme (LSVP) is a universal, specialist-delivered primary prevention programme for Year 9 pupils (aged 13 - 14 years), designed to improve attitudes towards harmful behaviours in dating and relationship contexts.

This project will evaluate the effectiveness of the LSVP in improving adolescents' attitudes towards harmful relationship behaviours. A two-armed cluster randomised controlled trial will be conducted with mainstream secondary schools across Greater London, with schools as the unit of randomisation. The primary outcome is pupils' attitudes towards harmful behaviours in dating and relationship contexts. An integrated mixed-methods implementation and process evaluation will examine implementation, mechanisms of change and contextual influences. Longer-term Police National Computer data linkage will explore DRV perpetration and victimisation. The study will provide evidence on whether universal, school-based education can improve adolescents' attitudes and contribute to the primary prevention of DRV.

ID: 210378

Start date: 01-10-2026

End date: 20-12-2028

Last modified: 17-09-2026

Grant number / URL: OC-EVAL-022602

Copyright information:

The above plan creator(s) have agreed that others may use as much of the text of this plan as they would like in their own plans, and customise it as necessary. You do not need to credit the creator(s) as the source of the language used, but using any of the plan's text does not imply that the creator(s) endorse, or have any relationship to, your project or proposal

# London Sexual Violence Project

## Manchester Data Management Outline

1. Will this project be reviewed by any of the following bodies (please select all that apply)?

- Funder
- Ethics

2. Is The University of Manchester collaborating with other institutions on this project?

- Yes - Part of a collaboration and owning or handling data

This project involves a collaboration between the University of Manchester (UoM), the University of Bristol (UoB), Brook (delivery partner), and Youth Endowment Fund (YEF; the funder of this project).

UoM will retain control of, and store, project data within its approved secure systems, detailed below. Where a named collaborator based outside UoM requires data to undertake a specified evaluation work package, UoM will provide access to the minimum necessary pseudonymised data through UoM-controlled systems. This will involve either: (a) a DSA between the UoM and collaborator's institution; or (b) making the named person an honorary member of staff at UoM to facilitate access to UoM systems (this will circumvent the need for inter-institutional data sharing). A minimisation process will be followed - access will only be provided to data needed to fulfil a given role/work package. Direct identifiers and the participant-linkage file will remain separately stored and accessible only to the trial manager and other specifically authorised UoM staff.

3. What data will you use in this project (please select all that apply)?

- Acquire new data
- Re-use existing data (please list below)

The following existing data relating to pupils will be collected from participating schools: first name, surname, date of birth, unique pupil number (UPN), sex, ethnicity, special educational needs (SEN) provision, SEN primary need (if applicable), and free school meal eligibility.

Demographic data will also be collected from pupils in surveys, including special category personal information (gender identity and sexual orientation).

New data will be generated through pupils' responses to survey questions, including: measures of attitudes towards harmful behaviours in adolescent dating and relationship contexts, pro-social behaviour, informal and professional help-seeking intentions, and knowledge of healthy relationships.

New data relating to process and implementation will be collected from school staff, Brook LSV Education and Wellbeing Specialist(s) working with the school, and pupils. This will include interview and focus-group audio recordings and transcripts, observation notes, staff and pupil feedback, delivery and implementation logs, usual-practice survey responses, documents such as school RSE policies, and participant-generated materials such as zines.

4. Where will the data be stored and backed-up during the project lifetime?

- University of Manchester Research Data Storage Service (Isilon)

Data will be kept in an encrypted Veracrypt container/folder (AES-256 algorithm), in a protected folder in Isilon. Access to the data requires 2FA to log into the University of Manchester network. The folder with the VeraCrypt file can only be accessed by

named users, and the container is itself protected with a long password (30+ characters, changed annually).

The exception to the aforementioned storage process concerns the fully anonymised interview and focus groups transcripts. Although these will be stored in the encrypted container described above, during the qualitative analysis process the research team members responsible for analysis of the transcripts will store them in the UoM managed LSV Microsoft Teams channel, which is restricted to the project team members and is equivalent to the UoM managed Microsoft 365 SharePoint channel. Once the qualitative analyses are complete, the transcripts will be deleted from the Teams channel and stored only in the encrypted drive within Isilon. The separate storage process for the interview and focus group transcripts is due to the fact that only one person can access the encrypted drive at one point in time, which would then preclude simultaneous analysis of said transcripts by different team members. Access to an encrypted drive may also require some team members to contact IT due to technical aspects, which could cause delays in storing data securely. This separate storage process allows the research team to still uphold the anonymity of the data, while preventing data analysis delay.

The encrypted container noted above is stored on an access restricted data share on UoM network storage infrastructure which is the recommended location for storing sensitive or critical UoM data. The storage infrastructure is hosted across two data centres approx. 4KM apart for resilience and disaster recovery purposes. Physical access to the data centres is strictly limited to data centre staff and a limited number of authorised IT Services staff. The data centres are protected by physical and electronic access security systems, swipe card access in and out of the data centres and CCTV coverage. The data centres are locked down out of hours and access is discouraged, but can be arranged by prior agreement with the data centre manager.

The UoM IT Services utilises Legato Networker Backup domains. Supporting infrastructure comprises disk libraries and both physical and virtual tape libraries. Cross data centre backup is performed, so services hosted within data centre 1 Joule House are backed up to data centre 2 Reynold House and vice versa. Backup/recovery plans are documented as part of the service install process during the commissioning of a specific service. Each Service is responsible for its business continuity and disaster recovery plans, to which IT Services feed in its technical recovery plans. ITSD operates change and release management processes. All proposed changes to infrastructure hosted, maintained and administered by IT Services are recorded via the Request for Change (RFC) process with changes being reviewed and authorised by a Change Advisory Board (CAB). Research data storage is not backed up to tape in the traditional fashion. However, resilience is obtained through replication and use of snapshots means that files deleted by accident or corrupted can be recovered. Hourly backups can be accessed within 24 hours and daily backups can be accessed within 35 days.

5. If you will be using Research Data Storage, how much storage will you require?

- 1 - 8 TB

6. Are you going to be receiving data from, or sharing data with an external third party?

- Yes

Data will be received from schools: schools will provide UoM with pupil background data, including unique pupil reference number (UPN), name, date of birth, sex, ethnicity, special educational needs and disabilities (SEND) and free-school-meal eligibility (FSMe), under a school-UoM data-sharing agreement (DSA). This data will be transferred to an authorised named recipient via ZendTo at specific timepoints in the trial. ZendTo encrypts files during network transfer. The sender will use the “Encrypt file” function, so that files can only be accessed using a separate passphrase. The passphrase will be communicated to the named authorised recipient through a separate channel (telephone). Access to ZendTo is controlled and logged. Uploaded files are retained for a maximum of 14 days and are then automatically deleted; ZendTo does not create backup copies of uploaded files. Schools will receive aggregate feedback only, unless a distinct lawful basis and arrangement permits more (for example, in the event of safeguarding concerns).

The Data Recipient (member of research team at UoM) will ensure that:

1. The data are only stored and processed in a secure networked environment controlled by UoM;
2. Where laptops are used to access the data, the laptops have full disk encryption and are solely connected to a secure networked environment within UoM IT infrastructure;
3. The data are stored only on computer systems where access to the data are limited by password protected individual user accounts and only authorised employees and students of UoM have access to such accounts;
4. Access to the data are provided only to authorised employees and students of UoM working on the trial;
5. Authorised employees and students of UoM with access to the data keep passwords and usernames confidential and do

not disclose or share those with any other person;
6. Current anti-virus and anti-malware software is installed on all systems and hardware being used to store or access the data.

The datasets generated during and/or analysed during the trial will be shared with the Department for Education (DfE) and Office for National Statistics (ONS), for storage in the Youth Endowment Fund (YEF) Data Archive for future research purposes. This includes pupils' names, gender, date of birth, UPN, and the unique reference number (URN) of the school the pupil attends. Two datasets will be created and submitted separately to the DfE and ONS:

1. One dataset containing just children's identifying data and a unique project specific reference number for each child will be submitted to the DfE, who will pseudonymise the data. In this process, the personal identifying data will be removed and replaced with DfE's pupil matching reference numbers (PMRs). The PMRs and the project specific reference numbers are then submitted to the ONS for storage in the YEF archive and deleted from the DfE system.
2. A second dataset containing the evaluation data and the project specific reference numbers will be submitted directly to the ONS, where it is also stored in the YEF archive.

Once the data has been submitted to the DfE and the ONS, the YEF will become the controllers.

Data from the National Pupil Database (NPD) will be accessed through a secure online environment, as facilitated by the Office for National Statistics (ONS). The research team will aim for remote access to NPD data with the ONS approved secure room located in the Ellen Wilkinson Building as a backup for accessing said data. The necessary steps for requesting access to said data will be followed and the relevant data sharing/data transfer agreements will be set up. The research team will lean on the expertise of the Information Governance team at the UoM.

After completion of the trial, the research team will share an anonymised version of the dataset on the Open Science Framework (OSF) website (or alternative established repository, given that the OSF are ceasing this service in early 2027) so that other researchers and organisations can use it. Before deposit, the research team will ensure that the dataset does not contain direct identifiers or other information that could enable identification of individual participants.

7. How long do you intend to keep your data for after the end of your project (in years)?

- 5 - 10 years

Project data will be deleted securely five years post project (i.e., in March 2034).

Guidance for questions 8 to 13

Highly restricted information defined in the Information security classification, ownership and secure information handling SOP is information that requires enhanced security as unauthorised disclosure could cause significant harm to individuals or to the University and its ambitions in respect of its purpose, vision and values. This could be: information that is subject to export controls; valuable intellectual property; security sensitive material or research in key industrial fields at particular risk of being targeted by foreign states. See more examples of highly restricted information.

If you are using 'Very Sensitive' information as defined by the Information Security Classification, Ownerships and Secure Information Handling SOP, please consult the Information Governance Office for guidance.

Personal information, also known as personal data, relates to identifiable living individuals. Personal data is classed as special category personal data if it includes any of the following types of information about an identifiable living individual: racial or ethnic origin; political opinions; religious or similar philosophical beliefs; trade union membership; genetic data; biometric data; health data; sexual life; sexual orientation.

Please note that in line with data protection law (the UK General Data Protection Regulation and Data Protection Act 2018), personal information should only be stored in an identifiable form for as long as is necessary for the project; it should be pseudonymised (partially de-identified) and/or anonymised (completely de—identified) as soon as practically possible. You must obtain the appropriate ethical approval in order to use identifiable personal data.

8. What type of information will you be processing (please select all that apply)?

- Special category personal data, or criminal offence data
- Personal information, including signed consent forms

- Anonymised personal data
- Pseudonymised personal data
- Audio and/or video recordings

1. Personal information to be processed (including in signed consent forms):

- First name, surname, date of birth, unique pupil number (UPN), sex, and free school meal eligibility. Participants' survey responses relating to attitudes towards harmful behaviours in adolescent dating and relationship contexts, pro-social behaviour, help-seeking intentions and knowledge of healthy relationships will also be processed.
- All of this information will be stored in accordance to the details provided in item 4.
- The project also involves opt-out parental/carer consent. These forms contain personal information (e.g. forenames, surnames) and may be received via postal delivery at various points in the project lifespan. Those forms will be kept in a locked drawer in B4.10 in the Ellen Wilkinson Building. A door code is required to access this office.

2. Special category personal data to be processed:

- Ethnicity, special educational needs (SEN) provision, SEN primary need (if applicable), gender identity, and sexual orientation.
- All of this information will be stored in accordance to the details provided in item 4.

3. Pseudonymised personal data:

- Statistical modelling will be implemented using pseudonymised personal data, to ensure accurate assessment of the programme's effectiveness.
- Qualitative analyses will utilise pseudonymised personal data relating to implementation and effectiveness of the programme but will not allow re-identification of participants (both pupils and staff).

4. Anonymised personal data:

- The 'public' version of the project dataset will be a completely anonymised version which will not allow re-identification of participants (both pupils and staff).
- Aggregate pupil anonymised data will be provided via reports to schools in tabular and data visualisation formats. The data will be provided in a way that prevents the re-identification of participating pupils. Measures are built into the reports to prevent disclosing information to schools with fewer than 10 participating pupils, per ONS disclosure guidance.

5. Audio recordings:

- Qualitative data will be generated as described in item 3. Audio recordings will be obtained either in person, using UoM managed audio recorders, or via UoM managed Microsoft Teams, which requires access clearance and dual factor authentication.
- Although video will be enabled during the interview, only audio will be recorded.
- The audio recording will then be stored in the encrypted VeraCrypt container/folder (AES-256 algorithm) in Isilon (as described in item 4).
- Audio recorded on audio recorders will be uploaded to the encrypted VeraCrypt container/folder and deleted from the recorder as soon as possible following data collection.
- The research team will abide by UoM Standard Operating Procedures regarding recordings of participants for research projects.

9. How do you plan to store, protect and ensure confidentiality of any highly restricted data or personal data (please select all that apply)?

- Store data in buildings, rooms or filing cabinets with controlled access
- Store data on University of Manchester approved and securely backed up servers or computers
- Store data on servers, computers or devices not connected to an external network
- Store data in encrypted files, folders, computers or devices
- Pseudonymise data and apply secure key management procedures
- Anonymise data
- Impose suitable data sharing and collaboration agreements
- Where needed, follow University of Manchester guidelines for disposing of personal data
- Access data hosted by the University of Manchester via its secure Virtual Private Network (VPN)
- Impose suitable non-disclosure agreements (e.g. for managers or users of personal data)

Data will be kept in an encrypted Veracrypt container/folder (AES-256 algorithm), in a protected folder in Isilon. Access to the

data requires 2FA to log into the University of Manchester network. The folder with the VeraCrypt file can only be accessed by named users, and the container is itself protected with a long password (30+ characters, changed annually).

The exception to the aforementioned storage process concerns the fully anonymised interview and focus groups transcripts. Although these will be stored in the encrypted container described above, during the qualitative analysis process the research team members responsible for analysis of the transcripts will store them in the UoM Microsoft LSV Microsoft Teams channel, which is restricted to the project team members and is equivalent to the UoM Microsoft SharePoint channel. Once the qualitative analyses are complete, the transcripts will be deleted from the Teams channel and stored only in the encrypted drive.

1. Store data in buildings, rooms or filing cabinets with controlled access:

- Room B4.10 in the Ellen Wilkinson building will contain the locked filing cabinets where opt-out consent forms and audio recorders are stored (although audio recorders will have their data uploaded to a secure setting and subsequently deleted as soon as possible). This room is locked and can only be accessed using a code, and the filing cabinet can only be accessed with a separate key.

2. Store data on University of Manchester approved and securely backed up servers or computers:

- All data will be stored on servers that are UoM approved, as described in item 4. These are securely backed up.

3. Store data in encrypted files, folders, computers or devices:

- All electronic and audio data will be kept in an encrypted VeraCrypt container/folder (AES-256 algorithm), in a protected folder on Isilon, as described in item 4.

4. Pseudonymise data and apply secure key management procedures:

- Qualitative and statistical analyses will utilise pseudonymised personal data.
- This will not allow re-identification of participants (both pupils and staff).
- Identifiable personal data (e.g. forename, surname) will only be kept for as long as is necessary to meet project objectives, after which it will be destroyed. Once all relevant analyses are completed, anonymisation will ensue.
- The required keys to transform pseudonymised data into identifiable data will be stored within the encrypted VeraCrypt drives, within UoM shared folders that require access clearance and dual factor authentication.

5. Anonymise personal data:

- The 'public' version of the project dataset will be a completely anonymised version which will not allow re-identification of participants (both pupils and staff). Before deposit, the research team will ensure that the dataset does not contain direct identifiers or other information that could enable identification of individual participants.
- Aggregate pupil anonymised data will be provided via reports to schools in tabular and data visualisation formats. The data will be provided in a way that prevents the re-identification of participating pupils. Measures are built into the reports to prevent disclosing information to schools with fewer than 10 participating pupils, per ONS disclosure guidance.

6. Impose suitable data sharing and collaboration agreements.

- Data sharing agreements (DSAs) with relevant parties (e.g. participating schools) will be set up. DSAs are fully GDPR (2018) compliant and reviewed by the UoM contracts team to ensure they meet the required standard.
- Contracts outlying the responsibilities of non-UoM team members will be implemented between the UoM and the team members' respective institutions.
- Access data hosted by the UoM via its secure Virtual Private Network (VPN). All participant data stored in the UoM folders will require VPN access.

7. Where needed, follow University of Manchester guidelines for disposing of personal data:

- The research team will seek the support of UoMIT services to ensure that destruction/disposal of personal data meets the required standard.

8. Access data hosted by the University of Manchester via its secure Virtual Private Network (VPN).

- All participant data stored in the UoM folders will require VPN access.
- Only authorised employees and students of UoM have access to those folders.

10. If you are storing personal information (including contact details) will you need to keep it beyond the end of the project?

- Yes – Other

The research team plan to store personal information beyond the end of the project (March 2029). Data will be stored securely (as detailed in item 4) up to five years post-project (i.e. March 2034). This is to maximise the potential for further insights resulting from the research and to enable data linkage to other government datasets (e.g., criminal justice information from the Police National Computer, or educational data in the National Pupil Database, as described in item 13). There are common delays to the process of data linkage to government datasets.

11. Will the participants' information (personal and/or sensitive) be shared with or accessed by anyone outside of the University of Manchester?

- Yes - Private organisations with contractual arrangements
- Yes - Public institutions with contractual arrangements (e.g. NHS research sites or other higher education institutions)

Participants' information will be shared with YEF, DfE and ONS, as detailed in item 6, by contractual agreement.

YEF is an independent charitable trust (registered charity no. 1185413) and the study funder; it is publicly funded but is not a public-sector authority.

Pseudonymised data will be shared with Prof Claire Fox (Co-Investigator) from the University of Bristol for the purposes of analysis. UoM will provide access to the minimum necessary pseudonymised data through UoM-controlled systems. This will involve either: (a) a DSA between the UoM and University of Bristol; or (b) making Claire Fox an honorary member of staff at UoM to facilitate access to UoM systems (this will circumvent the need for inter-institutional data sharing). A minimisation process will be followed - access will only be provided to data needed to fulfil a given role/work package. Direct identifiers and the participant-linkage file will remain separately stored and accessible only to the trial manager and other specifically authorised UoM staff.

Participating schools will be provided with a feedback report containing aggregated data in tabular and data visualisation formats. This will be completely anonymised and will not allow re-identification of participations. A failsafe will be built into the reports such that summary statistics are not calculated for any output representing fewer than 10 participants, per ONS disclosure guidelines.

Note: some schools (e.g. fee-paying independent schools may be private institutions).

12. If you will be sharing personal information outside of the University of Manchester will the individual or organisation you are sharing with be outside the EEA?

- No

13. Are you planning to use the personal information for future purposes such as research?

- Yes

We plan to link project data (e.g., forename, surname, unique pupil number, date of birth) to other government datasets (e.g., criminal justice information from the Police National Computer, or educational data in the National Pupil Database).

The purpose of the data linkage work is to maximise the potential for further insights resulting from the research (e.g. to examine whether LSVP has any longer-term effects; for example, whether it leads to reduced dating and relationship violence in young adulthood).

Accordingly, the data linkage strategy is clearly outlined in relevant documentation (e.g. parent/carer participant information and consent sheets).

14. Will this project use innovative technologies to collect or process data?

- No

15. Who will act as the data custodian for this study, and so be responsible for the information involved?

Prof. Neil Humphrey

16. Please provide the date on which this plan was last reviewed (dd/mm/yyyy).

2026-09-16

## Project details

What is the purpose of your research project?

This purpose of the project is to evaluate the effectiveness of the London Sexual Violence Programme (LSVP) in improving adolescents' attitudes towards harmful relationship behaviours.
LSVP is a universal, specialist-delivered primary prevention programme for Year 9 pupils (aged 13 - 14 years), designed to improve attitudes towards harmful behaviours in dating and relationship contexts.
The study will provide evidence on whether universal, school-based education can improve adolescents' attitudes and contribute to the primary prevention of DRV.

What policies and guidelines on data management, data sharing, and data security are relevant to your research project?

UoM Research Data Management Policy: http://documents.manchester.ac.uk/DocuInfo.aspx?DocID=33802%20
UK Concordat on Open Research Data: https:/ /www.ukri.org/about-us/policiesstandards-and-data/good-research-resource-hub/open-research/
UoM Data Protection Policy: https://documents.manchester.ac.uk/DocuInfo.aspx?DocID=14914
UoM Records Retention Policy: https://documents.manchester.ac.uk/DocuInfo.aspx?DocID=6514
UoM Information Security Policy: https://documents.manchester.ac.uk/display.aspx?DocID=6525
https:/ /documents.manchester.ac.uk/DocuInfo.aspx?DocID=6525
UoM Information Governance Accountability and Assurance Policy: https://documents.manchester.ac.uk/DocuInfo.aspx?DocID=8039
UoM Acceptable Use of IT facilities and Services: https://documents.manchester.ac.uk/DocuInfo.aspx?DocID=16221
UoM Standard Operating Procedures for Students: https://documents.manchester.ac.uk/display.aspx?DocID=16220
Data Protection Act/ GDPR (2018): https://www.legislation.gov.uk/ukpga/2018/12/contents
Freedom of Information Act (2000): https://www.legislation.gov.uk/ukpga/2000/36/contents
Youth Endowment Fund (YEF) Data protection information for YEF evaluations: https://youthendowmentfund.org.uk/wp-content/uploads/2023/11/YEF_Data_Protection_Evaluators-Oct-2023.pdf
Youth Endowment Fund (YEF) Evaluation Data Archive: https://youthendowmentfund.org.uk/evaluation-data-archive/:

## Responsibilities and Resources

Who will be responsible for data management?

Suzanne Hamilton will be responsible for data management as trial manager.

What resources will you require to deliver your plan?

For working remotely and at the office, team members will need a UoM managed laptop/desktop, a fast and stable internet connection, VPN access to the shared network, and a telephone number linked to the LSV Teams channel to provide passwords for files via phone, as outlined above.

## Data Collection

What data will you collect or create?

1. Data relating to pupils will be collected from participating schools:

- First name, surname;
- Date of birth;
- Unique pupil number (UPN);
- Sex;
- Ethnicity;
- Special educational needs (SEN) provision;
- SEN primary need (if applicable);
- Free school meal eligibility.

2. Demographic data relating to pupils will also be collected from pupils in surveys:

- Gender identity;
- Sexual orientation.

3. Data will be created/ collected from pupils via survey responses in relation to:

- Attitudes towards harmful behaviours in adolescent dating and relationship contexts;
- Pro-social behaviour;
- Informal and professional help-seeking intentions;
- Knowledge of healthy relationships;
- Relevant RSE coverage (in T1 surveys).

4. Data will be created/collected from school staff in all participating schools:

- Usual practice surveys completed by all participating schools at baseline/T0 and T1 spanning instructional elements (how RSE is taught) and practice elements(what RSE is taught);
- Surveys of relevant RSE coverage in T1 pupil surveys;

5. Data will be created/collected from school staff and Brook LSV Education and Wellbeing Specialist(s) working with intervention schools, relating to intervention implementation and process:

- Implementation logs and any other routine quality assurance data generated by LSVP Education and Wellbeing Specialists;
- Bespoke data items as required to build a comprehensive assessment of delivery in each school (e.g., reach, dosage) and cost calculations;
- Brook's existing evaluation survey that young people complete at the end of each session (no personal information is collected on this survey; this is anonymous).

How will the data be collected or created?

1. Data described in (1) above will be created/ collected in password protected excel files, sent from the school using the UoM ZendTo service, following the procedure detailed in item 6 of this DMP.

2. Data described in (2) and (3) above will be created/ collected in pupil surveys.
3. Data described in (4) above will be created/ collected in staff surveys:

- Usual practice surveys completed by all participating schools at baseline/T0 and T1 spanning instructional elements (how RSE is taught) and practice elements(what RSE is taught);

4. Data described in (5) above will be created/ collected in case studies of 8 of the participating intervention schools:

- Implementation logs and any other routine quality assurance data generated by Brook LSVP Education and Wellbeing Specialists;
- Bespoke data items as required to build a comprehensive assessment of delivery in each school (e.g., reach, dosage) and cost calculations;
- Brook's existing evaluation survey that young people complete at the end of each session (no personal information is collected on this survey; this is anonymous);
- Focus groups with pupils (up to 6 groups, approx. 48 young people per school);
- Interviews with the Brook LSV Education and Wellbeing Specialist(s) working with the school;
- Interviews with teachers and senior leaders (e.g., school PHSE leads) (N ≈ 6 per school);
- Observations of LSVP being delivered (1 of each of the 4 sessions in each school while avoiding one whole group being observed on multiple occasions);
- Observation of the 2-hour staff training session;
- Document analysis of relevant school policies (e.g., usual RSE provision).

5. Data from the National Pupil Database (NPD) will be accessed through a secure online environment, as facilitated by the Office for National Statistics (ONS). The research team will aim for remote access to NPD data with the ONS approved secure room located in the Ellen Wilkinson Building as a backup for accessing said data. The necessary steps for requesting access to said data will be followed and the relevant data sharing/data transfer agreements will be set up. The research team will lean on the expertise of the Information Governance team at the UoM.

All quantitative survey data will be created by means of online surveys using Qualtrics, a GDPR compliant platform. Qualitative data will be obtained either face to face, via semi-structured interviews and focus groups, using audio recorders, or using UoM managed Microsoft Teams (following the data storage procedures described in item 8).

Steps will be undertaken to ensure accurate data versions and versions of all ethics documentation.

## Documentation and Metadata

What documentation and metadata will accompany the data?

A codebook/data dictionary will accompany the quantitative dataset. This will clearly outline the contents, structure, and layout of the quantitative pupil dataset, and will draw on appropriate guidance (e.g. https://www.kuleuven.be/rdm/en/guidance/use-cases/case4-codebook-guidance.pdf
and
https://ies.ed.gov/ncee/rel/regions/central/pdf/CE5.3.2-Guidelines-for-a-Codebook.pdf
In order to be self-explanatory and unambiguous, the codebook will delineate as follows:

- Variable name (e.g. name or number assigned to each variable);
- Variable label (e.g. brief description to identify the variable for the user);
- Timepoint of collection;
- Question text (e.g. exact wording from survey question);
- Values (e.g. actual coded values in the data for this variable, such as 1, 2, 3, 4, 5);
- Value labels (e.g. textual descriptions of the codes, such as Excellent, Very Good, Good, Fair, Poor);
- Summary statistics where appropriate (e.g. unweighted summary statistics for quick reference);
- Missing data (e.g. the values and labels of missing data);
- Universe skip patterns where applicable (e.g. information about the population to which the variable refers, as well as the preceding and following variables);
- Notes: Additional notes that contextualise the information conveyed in a variable or relay special instructions.

Survey instruments, data-collection guidance, a data-processing and linkage record, and version-controlled analysis code with readme documentation will also be retained.

Qualitative data will be accompanied by topic guides, observation templates, transcription conventions and a coding

framework/codebook, including definitions of codes/themes and records of analytic decisions.
Documentation accompanying archived or shared data will exclude personal identifiers and linkage keys.

## Ethics and Legal Compliance

How will you manage any ethical issues?

The study was approved by University of Manchester Ethics Committee (UREC; REF 2026-25313-46597) on 13.04.2026. Below is an outline of ethical issues relevant to the study, and how they will be managed:
1. Consent and assent:

- Parent/carer opt-out consent and assent of young people completing the survey will be sought. This will be repeated prior to each annual data point (T0 and T1). The use of opt-out consent is absolutely standard for a trial of this nature, where the data being collected are extremely unlikely to trigger distress (although we will have a distress protocol - detailed below), involve minimal time burden (c.15 minutes, once per year), and no displacement of essential school activities (we anticipate completion during form-time). Evidence demonstrates that requiring explicit (i.e., opt-in) parent/carer consent reduces response rates and introduces selection biases, which affect the rigour and hence practical utility of the research.
- There is no legal requirement to seek explicit parent/carer consent for young people's involvement in research on non-medicinal intervention or observational studies and in line with the UoM general research privacy notice, we do not rely on explicit consent as our legal basis for processing participant data under GDPR (instead using public interest, and scientific research for special category data). See Bonell et al (2023): Approaches to consent in public health research in secondary schools, BMJ Open, for further information.
- Participating schools will use their electronic parent/carer engagement system (e.g. ParentMail or equivalent) to distribute information and consent documents. This is by far the most reliable means to ensure that parents/carers are informed about the study and have the opportunity to make an informed decision about their child's participation; indeed, schools use these systems to communicate critical information to all parents/carers.
- Participating schools will also be instructed to brief children so that they have at least 24 hours (preferably more) to decide whether to take part in the research. Briefing information will be included in the standardised instructions sent to schools, and will include a brief Powerpoint presentation (see Additional Documents; to note is that this includes instructions e.g. reminding school staff and pupils to respect privacy during survey completion) and short video (to be produced, but see example from one of our previous projects: https://www.youtube.com/watch?v=lGLbu1Uvx8w).
- Assent will be recorded directly in the survey process, i.e., young people will be presented with the participant information sheet at the front end of the survey and instructed to only click through to the survey itself if they would like to take part.

2. Confidentiality:

- Only the research team will access identifiable participant-level school and child data. Survey data will be kept in an encrypted Veracrypt container/folder (AES-256 algorithm) in Isilon, as outlined in item 4. Accessing to the data requires 2FA to log into the university's network. The folder with the Veracrypt file can only be accessed by named/approved users, and the container is itself protected with a long password (30+ characters, changed annually).
- School staff facilitating survey completion will be given a standardised set of instructions that reinforce each pupil's choice to participate (see Additional Documents). Those who opt not to do so (or who have been opted out by their parents/carers) will be given an alternative activity to complete, the nature of which will be decided by individual schools, but typically it is something of approximately the same estimated duration of survey completion (no more than 15 minutes for most young people) that can be completed at a computer so as not to draw attention to individual pupils.

3. Safeguarding and Disclosures:

- The participant information sheet for pupils completing the survey will be shown on the first page of the survey; it will remind them that the data they provide will not be used for screening purposes (e.g. their individual responses will not be shared with school staff and/or trigger any kind of referral process).
- Because all data generated from the pupil survey are fixed-response in nature (e.g. no open field options), it will not be possible for participants to make disclosures through the survey system.
- However, it is possible (though highly unlikely) that young people reveal information to a member of school staff following the completion of the survey, who will be reminded to follow their school disclosure protocol,and referral processes, in line with their safeguarding policy and procedures (see Distress and Disclosure protocol, section 20).
- The outcome survey completed by pupils does not include items that would reveal 'traditional' safeguarding issues (e.g. abuse, neglect, exploitation). A really important thing to note here is that we are measuring *attitudes* towards harmful

behaviours in adolescent dating and relationship contexts, NOT the behaviours themselves (i.e., we are *not* generating data that might indicate a young person is either a perpetrator or victim of DRV). While the topic of DRV overall is obviously somewhat sensitive, it is important to note that *all* secondary schools are *required* to cover it and related issues (e.g. consent, healthy vs unhealthy relationships, youth produced sexual imagery) as part of statutory Relationships and Sex Education (RSE). Hence, the behaviours covered in the survey are already included in discussions that take place in RSE lessons. The introductory text to the survey also very carefully frames the items to make clear that the attitudes represented are not being endorsed (i.e. "Please remember that these are just statements for research purposes and they are not advice or a guide on how people should act").
- Nonetheless, we have a clear distress protocol (see section 20: Distress and Disclosure Protocol) as part of our standardised instructions for school staff facilitating survey completion.
- Additionally, the survey will signpost young people to a range of sources of support that they can seek out (e.g. parent/carer, Childline, member of school staff) as required. Childline in particular offer a safe, confidential space to talk about anything, including relationship abuse (see Additional Documents - signposting will appear at the beginning and end of the survey).

4. Coercion:

- Our standardised instructions to school staff and the survey assent page will both reinforce children's rights to make their own decisions about whether or not to participate, and their right to withdraw at any time.
- As noted above, an alternative activity will be available for those who choose not to take part in the survey completion (or who have been opted out by parents/carers).
- Within the survey itself, young people receive regular reminders (at the start of each subsection) that they can skip any items that they don't want to answer.

5. Participant distress:

- A distress protocol will be in place and followed by the research team, setting out the steps we will take in the event a participant becomes distressed during the study, or will follow in the event a participant makes a disclosure that reveals they or others are at risk of harm.
- Where applicable, procedures for disclosures with a professional reporting obligation will be followed.
- If disclosures are made during the study that necessitate an exception to confidentiality (e.g., safeguarding, professional obligations), this will be documented, along with the specific actions taken, in accordance with safeguarding reporting guidelines.
- Adverse events will be reported on an Incident Response Form by the Principal Investigator and sent to Research Ethics, as per UoM policy.
- A debrief sheet will be provided to participants to share advice and information, such as signposting to appropriate support services.

A trial steering committee (TSC) and data monitoring and ethics subcommittee (DMEC) comprising approximately ten independent experts will also provide independent oversight of trial conduct and ethics. Meetings with the TSC-DMEC will take place three times each year throughout the duration of the trial.

How will you manage copyright and Intellectual Property Rights (IPR) issues?

Some measures used in our surveys may be subject to copyright and licensing arrangements, and so the research team will ensure compliance with these. The research team will obtain any necessary permissions for the use, adaptation, scoring, archiving or sharing of established measures.

Copyright and IPR for the new data and research materials generated by this project will rest with UoM, subject to any agreements with the funder and collaborators.

Copyright and IPR for existing data supplied by participating schools, and for any future linked data supplied by government bodies, will remain with the originating organisation.

Brook retains copyright and IPR in the LSVP intervention materials; these materials will not be shared, reproduced or deposited without Brook’s permission.

## Storage and backup

How will the data be stored and backed up?

Data will be kept in an encrypted Veracrypt container/folder (AES-256 algorithm), in a protected folder in Isilon. Access to the data requires 2FA to log into the University of Manchester network. The folder with the VeraCrypt file can only be accessed by named users, and the container is itself protected with a long password (30+ characters, changed annually).

The exception to the aforementioned storage process concerns the fully anonymised interview and focus groups transcripts. Although these will be stored in the encrypted container described above, during the qualitative analysis process the research team members responsible for analysis of the transcripts will store them in the UoM managed LSV Microsoft Teams channel, which is restricted to the project team members and is equivalent to the UoM managed Microsoft 365 SharePoint channel. Once the qualitative analyses are complete, the transcripts will be deleted from the Teams channel and stored only in the encrypted drive within Isilon. The separate storage process for the interview and focus group transcripts is due to the fact that only one person can access the encrypted drive at one point in time, which would then preclude simultaneous analysis of said transcripts by different team members. Access to an encrypted drive may also require some team members to contact IT due to technical aspects, which could cause delays in storing data securely. This separate storage process allows the research team to still uphold the anonymity of the data, while preventing data analysis delay.

The encrypted container noted above is stored on an access restricted data share on UoM network storage infrastructure which is the recommended location for storing sensitive or critical UoM data. The storage infrastructure is hosted across two data centres approx. 4KM apart for resilience and disaster recovery purposes. Physical access to the data centres is strictly limited to data centre staff and a limited number of authorised IT Services staff. The data centres are protected by physical and electronic access security systems, swipe card access in and out of the data centres and CCTV coverage. The data centres are locked down out of hours and access is discouraged, but can be arranged by prior agreement with the data centre manager.

The UoM IT Services utilises Legato Networker Backup domains. Supporting infrastructure comprises disk libraries and both physical and virtual tape libraries. Cross data centre backup is performed, so services hosted within data centre 1 Joule House are backed up to data centre 2 Reynold House and vice versa. Backup/recovery plans are documented as part of the service install process during the commissioning of a specific service. Each Service is responsible for its business continuity and disaster recovery plans, to which IT Services feed in its technical recovery plans. ITSD operates change and release management processes. All proposed changes to infrastructure hosted, maintained and administered by IT Services are recorded via the Request for Change (RFC) process with changes being reviewed and authorised by a Change Advisory Board (CAB). Research data storage is not backed up to tape in the traditional fashion. However, resilience is obtained through replication and use of snapshots means that files deleted by accident or corrupted can be recovered. Hourly backups can be accessed within 24 hours and daily backups can be accessed within 35 days.

How will you manage access and security?

Only named project staff will be able to access the project data. Accessing the data requires 2FA to log into the UoM network. The folder with the VeraCrypt file can only be accessed by named users, and the container is itself protected with a long password (30+ characters, changed annually). A minimisation process will be followed - access will only be provided to data needed to fulfil a given role/work package. Direct identifiers and the participant-linkage file will remain separately stored and accessible only to the trial manager and other specifically authorised UoM staff.

Survey data are collected via GDPR compliant Qualtrics, with results being exported directly into the above mentioned encrypted drive.

Qualitative data, in the form of audio recordings, will be collected following UoM standard operating procedures. Audio recordings from interviews conducted on UoM managed Microsoft Team will be uploaded to the encrypted VeraCrypt container/folder (AES-256 algorithm) in Isilon. Audio recorded on audio recorders will be uploaded to the encrypted VeraCrypt container/folder and deleted from the recorder as soon as possible following data collection.

Data received from schools will be transferred to an authorised named recipient via ZendTo at specific timepoints in the trial. ZendTo encrypts files during network transfer. The sender will use the “Encrypt file” function, so that files can only be accessed using a separate passphrase. The passphrase will be communicated to the named authorised recipient through a separate channel (telephone). Access to ZendTo is controlled and logged. Uploaded files are retained for a maximum of 14 days and are then automatically deleted; ZendTo does not create backup copies of uploaded files. Schools will receive aggregate feedback only, unless a distinct lawful basis and arrangement permits more (for example, in the event of safeguarding concerns).

The Data Recipient (member of research team at UoM) will ensure that:

1. The data are only stored and processed in a secure networked environment controlled by UoM;
2. Where laptops are used to access the data, the laptops have full disk encryption and are solely connected to a secure networked environment within UoM IT infrastructure;
3. The data are stored only on computer systems where access to the data are limited by password protected individual user accounts and only authorised employees and students of UoM have access to such accounts;
4. Access to the data are provided only to authorised employees and students of UoM working on the trial;

5. Authorised employees and students of UoM with access to the data keep passwords and usernames confidential and do not disclose or share those with any other person;
6. Current anti-virus and anti-malware software is installed on all systems and hardware being used to store or access the data.

## Selection and Preservation

Which data should be retained, shared, and/or preserved?

1. Data to be retained:

- The research team will retain the full project dataset, including pseudonymised survey, implementation and process-evaluation data, for as long as it is required to complete the trial (end date is end of March 2029), undertake agreed analyses, meet funder requirements, and facilitate the planned linkage and archiving processes.
- The research team plan to store personal information (e.g., forename, surname, unique pupil number, date of birth) beyond up to five years post-project (i.e. March 2034). Data will be stored securely, as detailed in item 4.
- This is to maximise the potential for further insights resulting from the research and to enable data linkage to other government datasets (e.g., criminal justice information from the Police National Computer, or educational data in the National Pupil Database, as described in item 13). There are common delays to the process of data linkage to government datasets.
- Once these purposes have been completed, or are no longer feasible, directly identifiable data will be securely destroyed following UoM guidelines.

2. Data to be shared:

- The datasets generated during and/or analysed during the trial will be shared with the Department for Education (DfE) and Office for National Statistics (ONS), for storage in the Youth Endowment Fund (YEF) Data Archive for future research purposes.
- This includes pupils' names, gender, date of birth, UPN, and the unique reference number (URN) of the school the pupil attends.
- Two datasets will be created and submitted separately to the DfE and ONS:
    - One dataset containing just children's identifying data and a unique project specific reference number for each child will be submitted to the DfE, who will pseudonymise the data. In this process, the personal identifying data will be removed and replaced with DfE's pupil matching reference numbers (PMRs). The PMRs and the project specific reference numbers are then submitted to the ONS for storage in the YEF archive and deleted from the DfE system.
    - A second dataset containing the evaluation data and the project specific reference numbers will be submitted directly to the ONS, where it is also stored in the YEF archive.
- Once those data have been submitted to the DfE and the ONS, the YEF will become the controllers.
- The research team will share an anonymised version of the dataset on the Open Science Framework (OSF) website (or alternative established repository, given that the OSF are ceasing this service in early 2027) so that other researchers and organisations can use it. Before deposit, the research team will ensure that the dataset does not contain direct identifiers or other information that could enable identification of individual participants.

What is the long-term preservation plan for the dataset?

The ONS will store the two datasets described above (i.e. that do not contain personal information) on the secure research service (SRS). Data managed in the SRS is governed by the ONS's 'Five Safes' framework. This data will be stored indefinitely.

More information about the longer-term preservation plan can be found in the YEF document 'Data protection information for YEF evaluations: Guidance for projects and evaluators (October 2023)': https://youthendowmentfund.org.uk/wp-content/uploads/2023/11/YEF_Data_Protection_Evaluators-Oct-2023.pdf

The research team will share an anonymised version of the dataset on the Open Science Framework (OSF) website (or alternative established repository, given that the OSF are ceasing this service in early 2027) so that other researchers and organisations can use it. Before deposit, the research team will ensure that the dataset does not contain direct identifiers or other information that could enable identification of individual participants.

## Data Sharing

How will you share the data?

Two datasets will be created and submitted separately to the DfE and ONS, as described above. In the future, approved researchers may apply to access YEF data via the ONS SRS.

The research team will share an anonymised version of the dataset on the Open Science Framework (OSF) website (or alternative established repository, given that the OSF are ceasing this service in early 2027) so that other researchers and organisations can use it. Before deposit, the research team will ensure that the dataset does not contain direct identifiers or other information that could enable identification of individual participants.

Are any restrictions on data sharing required?

The following restrictions on data sharing are required.

- Directly identifiable data, including names, dates of birth, UPNs, pupil-matching reference numbers (PMRs), or linkage keys, will not be made publicly available or shared outside the approved data-linkage and archiving arrangements described above. These data will only be transferred to the Department for Education (DfE) and Office for National Statistics (ONS) where necessary for the agreed YEF archiving and linkage process, and in accordance with the relevant data-sharing agreements and approved transfer procedures.
- A pseudonymised evaluation dataset, containing project-specific IDs, intervention information, participant characteristics/contextual information used in the evaluation will be deposited in the YEF Data Archive hosted by the ONS SRS, as described above. This dataset is not openly downloadable or publicly available. Future access will be restricted to researchers who are accredited by the ONS and approved by YEF. Access will be granted only for a specific research project that serves the public good, has appropriate ethical approval, and has been approved through the relevant ONS research-accreditation process.
- Researchers accessing the YEF archive will only have access to de-identified/pseudonymised data within the ONS SRS. They will not be permitted to remove record-level data from the secure environment. Any outputs must undergo ONS statistical-disclosure-control checking before release to ensure that individuals, schools, and other organisations cannot be identified.
- The separate, completely anonymised dataset that will be made publicly available through the OSF/ established repository will contain no direct identifiers, PMRs, linkage keys, school identifiers, or information that could reasonably permit re-identification. Data received from participating schools and any data obtained through future linkage to the National Pupil Database, Police National Computer, or other government sources will not be included in the public dataset.
- Participating schools will receive only aggregated feedback reports. Individual-level data will not be returned to schools. In accordance with the school data-sharing agreement, reports will include results only for groups of at least 10 pupils; no score or statistic will be reported for outputs representing fewer than 10 pupils.
- Qualitative data, including recordings, transcripts, observation notes, zines and other participant-generated materials, will not be shared publicly in raw form unless they have been assessed as genuinely anonymous, all potentially identifying material has been removed, and the consent arrangements explicitly permit such sharing. Given the risk of direct and indirect identification in small school-based samples, the default position will be that raw qualitative data remain restricted to the research team and any approved archiving arrangement.