

SAINT PAUL UNIVERSITY
Office of Research and Ethics (ORE)

OPERATIONAL GUIDE

Preventing Fraud in Research Participation

Prevention | Detection | Management | Ethical Compliance

Item	Information
Version	3.0 – Proposed final version
Date	September 2026
Status	Ready for adoption by the Research Ethics Board (REB)
Prepared by	Office of Research and Ethics (ORE)
Intended audience	Researchers, students, research supervisors, REB members and support services
Next review	No later than September 2027, or sooner if needed

Proposed institutional decision

Adopt as an operational guideline of the REB. This guide supports scientific and ethical judgment; it is neither a fraud diagnostic tool nor a sanctions policy.

Approval and document control

Body	Decision / date
Research Ethics Board	Adopted on: September 16, 2026
Administrative lead	Research and Ethics Office
Review cycle	Annually or upon a significant regulatory, technological or institutional change

Contents

1. Purpose, scope and guiding principles
 2. Definitions
 3. Understanding the risk
 4. Planning prevention
 5. Consent, privacy and metadata
 6. Detecting and assessing suspicious participation
 7. Managing suspicious or inauthentic cases
 8. Compensation and data handling
 9. Amendments and events to report to the REB
 10. Roles and responsibilities
 11. Implementation, documentation and review
- Appendices: operational tools and references

Quick reference

For any online study: plan controls before data collection, use multiple indicators, limit personal information, preserve data when concerns arise, and clearly distinguish scientific quality, compensation and obligations to the REB.

1. Purpose, scope and guiding principles

Inauthentic participation can undermine a study's scientific validity and, depending on the circumstances, raise ethical, privacy or security concerns. This guide helps research teams at Saint Paul University prevent, detect, assess and manage this risk proportionately.

The guide applies primarily to research involving humans conducted online or remotely, including surveys, questionnaires, virtual interviews, focus groups and public recruitment with compensation.

- The principal investigator remains responsible for the scientific conduct of the study, monitoring data collection and decisions about data quality.
- The REB assesses the ethical acceptability of the protocol, substantive amendments and events within its mandate.
- The ORE administers the process and provides guidance.
- Measures must be necessary, proportionate, equitable, accessible and documented.
- No signal, automated tool or AI detector is, on its own, proof of fraud.

Guiding principle

Protect data validity without collecting more personal information than necessary. Suspicious participation calls for review, not an accusation.

2. Definitions

Term	Operational definition
Inauthentic participation	Participation that does not come from an eligible person acting in accordance with the study's terms, particularly because of a material misrepresentation, prohibited multiple participation or automation.
Suspicious participation	Participation with one or more signals warranting review, without a prior conclusion about intent or authenticity.
Bot	An automated tool capable of submitting a form or generating responses without human participation consistent with the protocol.
Multiple participation	Multiple submissions by the same person when the protocol limits participation to one submission.
Metadata	Technical or contextual data associated with a submission, such as a timestamp, duration, IP address or certain device characteristics.
Analytical exclusion	A documented decision not to include certain data in the analysis, based on defined and justified criteria.
Unanticipated event	An event that may increase the level of risk to participants or have other ethical implications affecting their welfare.
Substantive amendment	A change to the approved protocol that may affect ethical acceptability, including recruitment, consent, verification, confidentiality or compensation.

3. Understanding the risk

Risk varies with recruitment methods, link accessibility, the target population, the amount and visibility of compensation, the nature of the data requested and the ability to verify eligibility. Artificial intelligence can facilitate plausible and distinct responses; it does not, however, permit an automatic conclusion that text was artificially generated.

3.1 Common forms

- Misrepresentation of an eligibility criterion;
- Automated submissions;
- Prohibited multiple participation;
- Impersonation or concealment of technical indicators;
- Fabricated responses or responses unrelated to the experience requested;
- Attempts to disrupt or manipulate data collection.

3.2 Risk-based approach

Indicative level	Example contexts	Recommended response
Low	Targeted recruitment, known population, no compensation or a modest incentive	Basic controls and periodic monitoring.
Moderate	Semi-public link, specialized criteria, individual compensation	Layered measures, prescreening and regular monitoring.

Indicative level	Example contexts	Recommended response
High	Public link, wide distribution, attractive compensation, sudden rise in responses	Enhanced plan, close monitoring, predefined review criteria and technical support.

4. Planning prevention

Measures should be selected before launch and described in the protocol when their scope is substantive. A reasonable combination of measures is preferable to a single control.

4.1 Recruitment and eligibility

- Where possible, limit distribution of data-collection links to relevant, traceable channels.
- Do not disclose nonessential details in a public notice that would allow prescreening to be circumvented; material criteria must nevertheless be communicated before consent or under an approved procedure.
- Use neutral, relevant prescreening questions without requesting more information than necessary.
- Provide an accessible alternative when the usual verification method is unsuitable for a legitimate participant.
- Avoid decisions based on demographic, linguistic, cultural or socioeconomic stereotypes.

4.2 Compensation and recruitment

- Choose compensation proportionate to the time, burden and context of the study.
- Avoid unnecessarily emphasizing the incentive amount in public notices, while providing the information required for informed consent before participation.
- Describe the method, amount, payment timeline and any objective eligibility conditions in approved documents.
- Do not require a physical address, camera or particular payment method as a general rule; any measure must be justified and approved.

4.3 Platforms and technical controls

- Use an institutionally approved platform and configure available protective features in accordance with the protocol.
- Consider multiple-submission prevention, automated-activity detection and response-quality features where available.
- Confirm with IT which features are actually included in the institutional licence and their privacy implications.
- Never let an automated filter alone trigger exclusion, non-payment or irreversible deletion.
- Keep technical instructions that may change rapidly separate from this guide, in a distinct IT fact sheet.

4.4 COMPASS framework

COMPASS is an SPU teaching aid. It organizes recognized practices but is neither a regulatory standard nor a validated detection instrument.

Component	Application
C – Consistency	Examine internal logic and relevant contradictions.
O – Open-ended questions	Use open-ended questions judiciously and adapt them to the population.
M – Multiple methods	Combine methodological, human, statistical and technical controls.
P – Patterns and trends	Examine trends without equating atypical with fraudulent.
A – Adaptation	Update controls and technical documentation.

Component	Application
S – Staged follow-up	Plan beforehand, monitor during collection and verify afterward.
S – Support and preparation	Train teams and define consultation pathways.

5. Consent, privacy and metadata

5.1 Transparency with participants

Depending on the nature of the study, consent documents should clearly explain:

- material eligibility criteria;
- the checks that will be performed;
- the categories of metadata collected and their purpose;
- the possible effects of exclusion on data use;
- compensation terms and timelines;
- limitations on anonymity or confidentiality arising from technical controls.

5.2 Metadata governance plan

Item	Minimum requirement
Purpose	Explain why each metadata item is needed.
Proportionality	Use the least intrusive reasonably effective method.
Link to responses	Limit and protect any link between metadata and responses.
Access	Identify authorized roles and apply the need-to-know principle.
Retention	Set a separate, justified retention period.
Destruction or unlinking	Specify the method and timing.
Provider and hosting	Document known factors relevant to ethical review.
Secondary use	Prohibited without an appropriate basis and approval.

Caution

An IP address or device characteristic may be identifying in context. A study must not be called anonymous if its controls can reasonably link a submission to a person.

6. Detecting and assessing suspicious participation

The indicators below warrant contextual review. Their strength depends on the design, recruitment, population and available reference data.

Indicator	Cautious interpretation
Sudden rise in volume	Check the recruitment channel, timing and content; a legitimate campaign can also cause a spike.
Unusual submission times	Contextual signal only; consider time zones, work schedules and participants' circumstances.
Very short duration	Compare with pilot testing or the observed distribution; legitimate participants may respond quickly.
Highly regular intervals	May suggest automation when it converges with other signals.
Repetitive, generic or off-topic text	Examine the question, literacy, language and accessibility before drawing conclusions.
IP, VPN, proxy or shared device	Inconclusive technical signal; households, institutions and shared networks can produce legitimate duplicates.
Unexpected response pattern	Check against approved criteria, without stereotyping or profiling.
Failure of an attention check	One failure alone establishes neither fraud nor malicious intent.

6.1 Decision rule

- Define criteria and thresholds before collection where possible.
- Normally seek multiple independent, converging indicators.
- Distinguish weak signals from evidence objectively establishing ineligibility.
- Where possible, have ambiguous cases reviewed by a second trained team member.
- Record the evidence reviewed, decision, rationale and date.

6.2 AI detectors

AI detectors may be used only as exploratory indicators. They should not be presented as reliable for establishing the origin of a text and must never be the sole basis for exclusion or non-payment.

7. Managing suspicious or inauthentic cases

1. Record the signal detected and preserve raw data, relevant logs and collection settings.
2. Place the affected data in logical quarantine, without irreversible deletion.
3. Apply the preapproved criteria and checks.
4. Where relevant, obtain an independent second review of the initial decision.
5. Determine separately the analytical treatment of the data, compensation and ethical obligations.
6. Consult the ORE if the institutional interpretation or REB process is uncertain.
7. Report promptly to the REB any situation meeting the criteria in section 9.

Cautious communication

Avoid accusing a participant of fraud. Use factual language, limit exchanges to necessary information and do not undertake an unapproved intrusive investigation.

7.1 Exclusion and retention

Analytical exclusion is the researcher's scientific responsibility, in accordance with the protocol and analysis plan. Suspicious data must be preserved long enough to allow review, traceability and, where applicable, institutional

verification. Irreversible deletion must comply with the protocol, data management plan and any applicable REB instruction.

8. Compensation and data handling

The decision about compensation is distinct from the decision about using the data. Analytical exclusion therefore does not automatically entail non-payment.

Situation	Data	Compensation
Ineligibility established before participation	Do not collect research data, except minimal information planned for prescreening.	According to approved terms; normally no participation has begun.
Voluntary withdrawal	Handle in accordance with consent and applicable withdrawal rules.	Pay any amount already owed; apply the approved flat-rate or staged structure.
Partial participation	Retain or remove according to consent and scientific value.	Apply approved and communicated terms.
Unresolved doubt	Quarantine and document; do not automatically conclude fraud.	Favor the planned payment to avoid disadvantaging a legitimate participant.
Inauthenticity sufficiently established	Exclude using objective, preapproved and documented criteria.	Any non-payment must be based on objective, proportionate, clearly communicated and approved conditions.
Researcher stops participation for reasons not attributable to the participant	Handle according to the protocol.	Do not deprive the participant of compensation earned or promised under approved terms.

9. Amendments and events to report to the REB

A data anomaly or inauthentic participation is not automatically a reportable event. The decision depends on ethical impact, risk and the need to amend the protocol.

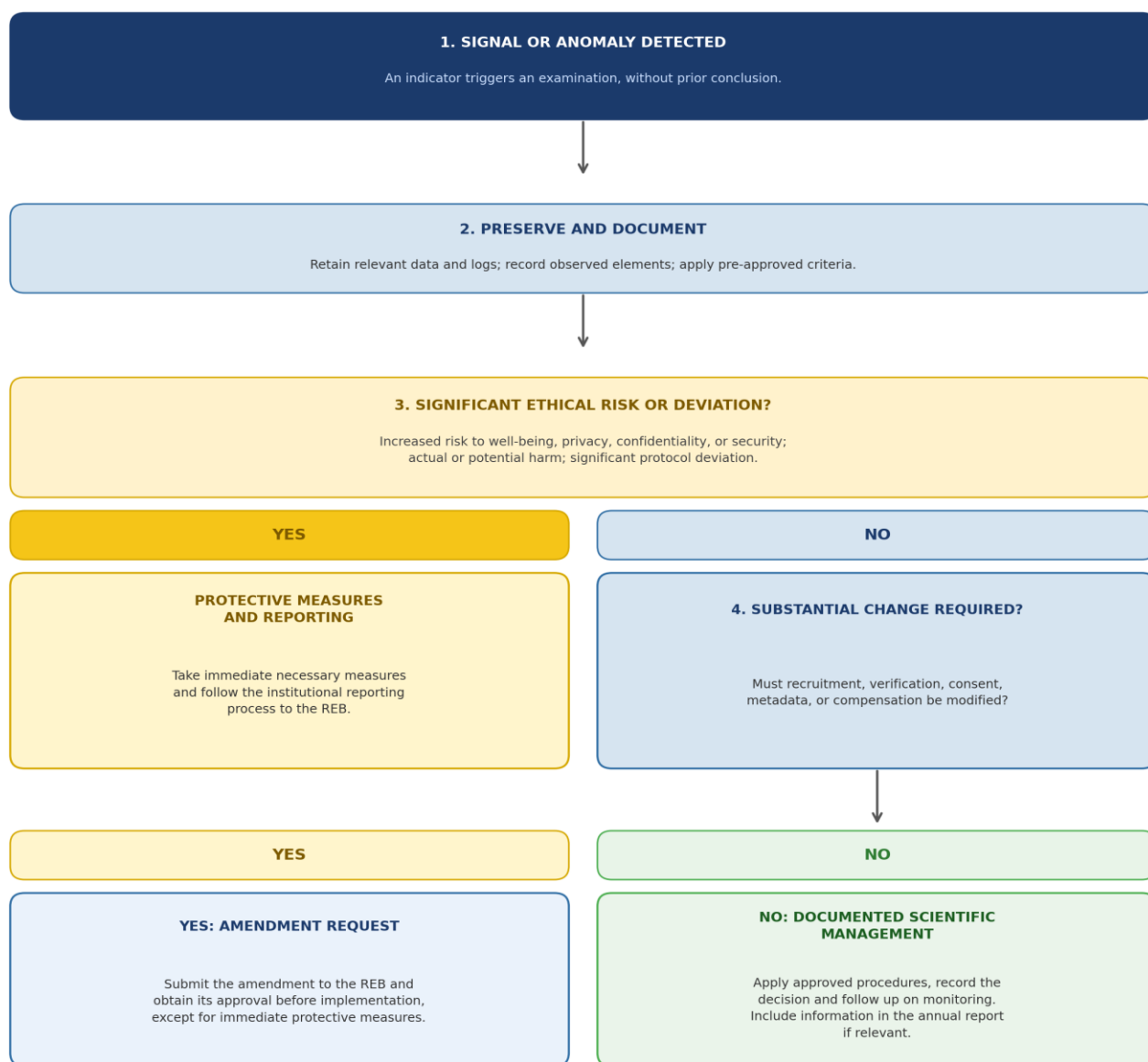
Situation	Course of action
Increased risk to participant welfare	Take immediately necessary protective measures and report promptly to the REB.
Actual or potential breach of privacy or confidentiality	Protect the information, consult the appropriate institutional functions and report to the REB under applicable procedures.
Significant protocol deviation	Consult the ORE and determine whether a report to the REB is required.
Substantive change to recruitment, verification, consent, metadata or compensation	Submit an amendment and obtain approval before implementation, except for an immediate measure needed for protection.
Exclusion under already-approved criteria, with no additional risk	Document in the research file and include in the annual report if relevant.
Unconfirmed suspicion with no additional risk	Documented scientific management; consult the ORE as needed.

9.1 Decision flow

Suspicious or inauthentic participation does not automatically require a protocol amendment or a report to the Research Ethics Board (REB). The appropriate response depends on the level of risk, potential ethical impact and measures needed to continue the research compliantly.

When a signal or anomaly arises, the researcher must first preserve the affected data and document the observations. The researcher must then determine whether the situation entails a risk to participants, privacy or confidentiality, or requires a substantive change to approved procedures. The decision points are outlined below.

Figure 1. Decision Flow for Managing Suspicious or Non-Authentic Participations



Note. The decision regarding data, compensation, and obligations toward the REB must be made separately. The BRD may be consulted when the appropriate path remains unclear.

Interpreting the decision flow

- **Ethical risk or significant deviation:** take appropriate protective measures and follow institutional procedures for consultation or reporting to the REB.
- **Substantive amendment:** obtain REB approval before changing recruitment, verification, consent, metadata or compensation, except for an immediate measure necessary for protection.
- **Documented scientific management:** if no additional risk or substantive change is identified, apply approved procedures, record the decision and continue monitoring.

GUIDING PRINCIPLE

Suspicious participation is not automatically an event reportable to the REB. Reporting depends on an ethical risk, a potential privacy or confidentiality breach, a significant protocol deviation or the need for further ethics approval.

10. Roles and responsibilities

For student projects, the student carries out activities under the supervision and scientific accountability required by the University.

Activity	Principal investigator	Research supervisor	REB	ORE	IT
Protocol design	A/R	C	C	C	I
Training and institutional tools	I	C	I	A/R	C
Prevention measures	A/R	C	C	C	C
Technical configuration	R	C	I	C	A/R
Monitoring data collection	A/R	C	I	I	I
Analysis and cleaning	A/R	C	I	I	I
Ambiguous cases	A/R	C	I	C	C
Event reporting	R	C	A	C	I
Protocol amendment	R	C	A	C	I
Privacy and metadata	A/R	C	A for ethical acceptability	C	C on technical matters

R = performs the work; A = accountable or grants the required approval; C = consulted; I = informed.

11. Implementation, documentation and review

11.1 Minimum research file

- Initial assessment of the risk of inauthentic participation;
- Measures selected and rationale;

- Relevant technical settings;
- Review and exclusion criteria;
- Log of signals and decisions;
- Record of consultations and communications;
- Decisions about data and compensation;
- Reports or amendments submitted to the REB.

11.2 Review of the guide

The ORE reviews the guide at least annually, or sooner when warranted by a significant regulatory, technological or institutional change. Platform-specific feature names and instructions are kept in a separate technical fact sheet.

Appendix A – Prelaunch checklist

- ☐ Risk assessed and documented
- ☐ Recruitment channels defined
- ☐ Material criteria communicated at the appropriate time
- ☐ Proportionate prescreening measures
- ☐ Compensation and timeline clearly described
- ☐ Metadata justified and disclosed
- ☐ Access, retention and destruction defined
- ☐ Technical features checked with IT
- ☐ Review and exclusion criteria predefined
- ☐ Procedure for ambiguous cases defined
- ☐ Documents and procedures approved by the REB where required

Appendix B – Recommended decision log

Date / code	Signal observed	Evidence reviewed	Second review	Decision and rationale	Data / compensation / REB

Appendix C – Sample consent language

Template to adapt

To protect study quality, the team may use measures to verify eligibility and response quality. These measures may include [describe]. The following technical information may be collected: [categories]. It will be used only for [purpose], accessible to [roles], retained for [period], then [destroyed or unlinked]. Only one participation per person is permitted. Compensation terms are as follows: [amount, method, timing and objective conditions]. An anomaly does not automatically lead to a finding of fraud.

Appendix D – Resources and references

- Canadian Institutes of Health Research, Natural Sciences and Engineering Research Council of Canada, and Social Sciences and Humanities Research Council. Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans, TCPS 2 (2022), particularly Chapters 3, 5 and 6.
- University of British Columbia, Behavioural Research Ethics Board. How to Mitigate Participants Falsifying Eligibility.
- University of Calgary, CFREB/CHREB. Preventing Fraudulent Participants – Guidance, version 1, March 2024.
- University of Alberta, Research Ethics Office. Fraudulent Participants Guidance, December 2025; adapted from the University of Calgary guide.
- University of Toronto, Centre for Research & Innovation Support. Guidance for Mitigating Fraud and Safeguarding Data Integrity in Online Research.
- University of Toronto. Compensation & Reimbursement of Research Participants.
- Qualtrics. Survey Protection and documentation on response-quality and multiple-submission prevention features. Consult current documentation and the SPU licence before use.
- Armstrong, L. AI in Research: Fake Participants, Automated Responses and Protecting Data Quality. Presentation at Saint Paul University, November 4, 2025.