DEPARTMENT OF
SCIENCE AND TECHNOLOGY STUDIES

STS guidance for research review

Research **cannot** be undertaken without necessary approvals in place prior to its start. Three areas are prescribed for STS-based research projects:

1. ethics of research methods, mandatory for research using humans as data
2. data protection, mandatory for research using personal data
3. safety and risk assessment, mandatory for off-site locations and lone working

These processes are recommended for all research activities. Without exception, all research at UCL involving "intervention or interaction with living human participants or the collection or study of data derived from living human participants" must receive ethical approval of methods *prior to the start* of data collection. UCL also requires approval of plans to protect certain types of data and to assess risks to safety.

Supervisors and line managers are responsible to ensuring projects under their direction meet all UCL requirements. STS RRP **strongly advises** staff and students to secure independent decisions about applicability. STS researchers should feel encouraged to discuss project and protocol design with their colleagues, supervisors, and line managers. In teaching, module tutors or supervisors are the first point-of-contact. Research students, research fellows, and other academic staff have recourse to research clusters, especially cluster leads. Our community has tremendous wealth of experience in areas of protocol design and engagement with responsible research.

To secure approvals, the institution has three pathways:

1. UCL REC: In these areas, UCL central processes are supreme, providing default systems. These are managed by UCL Research Ethics Committee (UCL REC). UCL offers training in all aspects of research preparation, including research ethics, data protection, and safety and risk management.

2. STS RRP: Because the central system can seem daunting, and because most STS research involves relatively low risk interventions or collection of non-personal data, STS maintains a streamlined screening process as a preliminary stage in review. The purpose of our local STS review is to identify, approve, and monitor low risk research and non-personal data collection. Most research involving more-than-minimum risk will be referred to UCL REC as a matter of routine.
   Research review within STS is managed by the STS Research Review Panel (RRP). For 2021-22, the lead is **Dr Jack Stilgoe.** All documentation, requests for approval, and reviews are managed by the STS Research and Finance Administrator, Ms Susan Walsh. Contact the panel via STS.Ethics@ucl.ac.uk. Information is online www.ucl.ac.uk/sts/ethics..

3. Other departments: STS researchers collaborating with colleagues in other UCL departments can use alternate review processes within UCL. Those collaborating with colleagues elsewhere should consult the STS RRP lead about comparability and transferability.

Applications to STS RRP

Use this form	which covers this area	because research involves
Consider methods	methods and protocols	humans as research subjects or information sources data collected from or about identifiable humans specific methods you believe merit independent review
Consider data	data protection and storage	personal data (as defined by GDPR) confidential information drawing boundaries about privacy long term decisions about management and storage
Consider safety	safety and risk assessment	humans as research subjects work outside UCL facilities lone working or out-of-hours working in UCL facilities specific risks you think are important

A. Step-by-step process

Steps towards approvals for research using humans as research subjects.

1. Discuss project with supervisor or line manager, and colleagues. Draft applications well in advance of need.

2. UCL REC provides the default process for approvals and for more-than-minimum risk activities.

3. STS RRP can screen applications and consider proposals which involve (1) no vulnerable groups, (2) minimum risk, and (3) in some limited cases, more-than-minimum risk. You need to submit all three forms (Consider methods, Consider data and Consider safety). All materials must be submitted through STS.Ethics@ucl.ac.uk

Applicants approved through UCL REC, or through other UCL departments, do not require STS RRP approval.

1. Key decisions to decide between UCL REC or STS RRP

UCL REC provides the default process for approvals and for most more-than-minimum risk activities. STS RRP can screen applications and consider proposals which involve (1) no vulnerable groups, (2) minimum risk, and (3) in some limited cases, more-than-minimum risk.

1.1 Does my project involve “vulnerable groups”?

A. Essential decision
Projects **proposing to involve vulnerable groups** are automatically referred to UCL REC, so researchers in this position should proceed directly to UCL REC. No STS screening is undertaken in such cases.
Projects **not involving vulnerable groups** may use either STS RRP or UCL REC processes. The choice is made by the project leader or supervisor.

B. Criteria for “vulnerable group”
Certain groups of people are designated “vulnerable” because external concerns exist about possibilities for exploitation by researchers, because certain limits might exist in a person’s selfdetermination,or owing to legal classification.

These groups include:

- children (anyone under 18 years old)
- adults with diminished mental, physical, or social capabilities
- adults with diminished power as decision makers in society (such as refugees or individuals who are homeless)
- adults with significant investments in certain outcomes of the research

Researchers must consult supervisors or line managers in cases where ambiguity exists as to the extent of “vulnerability”. A precautionary principle – presuming the category applies unless it is agreed unambiguously that it does not – functions as a default.

1.2 Does my data collection involve “minimum risk”?

A. Essential decision
Projects proposing **minimum risk** involvement of humans may use STS RRP processes.
Projects proposing **more-than-minimum risk** involvement of humans should use UCL REC processes by default. STS RRP processes can serve as an alternative in cases when timelines are short *and* when specific and straightforward risk management can be implemented. The project supervisor or line manager can advise on this decision.

B. Criteria for minimum risk involvement
Minimum risk involvement is predicted to leave no lasting negative impact on the research subject. Examples of minimum risk include:

a. Interviews to collect data about external events, activities, and information but avoiding questions about the participants themselves and avoiding invitations to reflect about themselves or introspect. Typical questions in this line are, “What happened?” “Who was involved?” “Who did what?” “What was your role?” “Why do you think this happened?” Such investigation is typical of journalism or fact-collecting external to the individual interviewed.

b. Questionnaires might involve short lists of closed questions presented in anonymised questionnaires. Such investigation is typical of a class evaluation or user survey. The NSS is an exemplar.

c. Data gathering might require only passive or ephemeral involvement of research subjects, such as data analysis of footfall patterns, crowd or published photographs, or data streams from open social media or analytics services. In these cases, the researcher plays an observer's role and makes no intervention. They do not change the course of events.

d. Opinion gathering might involve vox-pop style interviews of passing pedestrians who are asked a few open-ended questions in relation to topics of the day.

C. Criteria for more-than-minimum risk involvement

More-than-minimum risk involvement is predicted plausibly to leave some negative or otherwise powerful impact on the research subject as a consequence of their participation. Such impacts might involve additional distress, embarrassment, stigmatization, anxiety, introspection, guilt, renewed memories of difficult events, excessive anger, a feeling of a life permanently altered, etc. Powerful impacts might involve unusual levels of validation or restructuring of personal life narratives. Where there is plausible risk of either type of impact, steps must be taken towards mitigation and reduction. This can include methodological choices that are likely to dampen impact. It also can include amplified post-research support for processing impacts, such as post-research debriefing and reconciliation, or follow-up support.

Examples of more-than-minimum risk involvement include:

a. Interviews about failure, loss, distressing events, involvement in controversial activities, involvement in potentially illegal or unethical activities (e.g., hacking or trespass)

b. Questionnaires seeking introspection on protected characteristics as defined by the Equality Act (age, disability, gender reassignment, race, religion or belief, sex, sexual orientation, marriage and civil partnership and pregnancy and maternity)

c. Data gathering involving participant-observer ethnographies

d. Opinion gathering in sensitive settings (e.g., interview mourners in a cemetery about death)

e. Data collection from non-passive surveillance, non-public spaces (physical or digital), or law enforcement

f. Processing of data sets from third-party sources involving more-than-minimum risk data collection or where consent to original data collection either is ambiguous or cannot be demonstrated.

g. Data collection in which research subjects are recruited in non-random ways, or when intermediaries and facilitators (such as translators or community leaders) are significantly involved.

2.1 Using "Consider methods"

Research methods should be examined for their veracity (will they generate data meaningful to the research questions), their worthiness or beneficence (data sufficient to justify the effort of the research subjects), and their efficiency (the most data collection possible under the circumstances). For the most part, these are matters for researchers and supervisors to agree.

Ethics review of methods considers work in a wider frame. When humans are involved as research subjects, methods also must demonstrate basic principles of human rights and human dignity. Core principles relevant human research ethics are (1) autonomy, (2) dignity, and (3) privacy. No matter which research protocol is used, STS researchers are expected to use those which affirm such core principles. Crucially, review of methods must be done from a position of independence and detachment.

Screening of research proposals in STS is intended to identify projects that (1) use no vulnerable groups as research subjects, *and* (2) predict minimum risk to research subjects during data collection. Projects with more-than-minimum risk might also be considered within the department, especially when timelines are short *and* when specific and simple risk management can be implemented. Screening also is intended to quickly identify research proposals requiring UCL REC consideration.

A. Essential decisions

You must demonstrate a system for securing informed consent from your research subjects. You also must design research protocols that maintain core principles of autonomy, dignity, and privacy.

B. Managing informed consent

With rare exceptions, data collection involving humans cannot proceed without the **informed consent** of the people providing the information. Researchers must include in their protocols mechanisms for informing research subjects, mechanisms for securing consent, and mechanisms for documenting both processes.

B1. managing "informed"

A series of conventions and regulations define what research subjects should know about data collection prior to their participation.

As a minimum, researchers are expected to provide participants with the following information:

- who is responsible for the research and who is undertaking the data collection?
- what is the aim of the data collection?
- what does the data collection entail for the research subject?
- what are likely and predictable impacts from participation, and how are researchers managing risks?
- what will research subjects be told about the results from their participation or results from the project as a whole?
- who should participants contact with a query or to raise a concern?

Some protocols require more, and the application process will consider specifics on this point. Most relevant to STS, the collection of personal data is covered by GDPR and requires specific consents and positive opt-ins.

B2. using information sheets

An information sheet is a typical delivery mechanism for "informing" research subjects. A signed copy retained is a typical record of delivery. Care must be taken to ensure the appropriateness of language and instruction for the reader.

UCL REC offers templates. Other techniques are available and might be more suitable for some circumstances. Consult your supervisor or line manager of which template suits the purpose best.

Information sheets also typically include information regarding data processing and data protection.

B3. managing "consent"

Once informed about the project and its methods for data collection, research subjects must give their consent to participate. Consent must be free, explicit, and informed.

- "free" consent is free from coercion, social pressure, and intimidation. It also is free from reward and inducements.
- "explicit" consent is a positive opt-in agreement to participate. Participation cannot be set as a default action.
- "informed" consent requires knowledgeable decision-making.

STS will not approve proposals where research subjects are paid for their participation. (Apply through UCL REC in these cases.) However, STS will consider cases in which travel and catering expenses can be reimbursed assuming funds have been secured (such as in research grants).

Research subjects have an absolute right to withdraw their consent at any time, for any reason, and without penalty. Withdrawal must have a very low bar – simply stating a desire to withdraw must be sufficient. On withdrawal, research subjects must have the opportunity to decide what is to be done with data collected to that point. Their decision must be sovereign regardless of the cost to data collection.

B4. using consent forms

A consent form is a typical document for securing "consent". A signed copy retained is a typical record of consenting. Care must be taken to ensure the appropriateness of language and instruction for the reader.

UCL REC offers templates. Key to a consent form is clarity about (1) right to withdraw and procedures for withdrawal, and (2) the processes of data collection directly involving the research subject.

Consent forms also typically include information regarding data processing and data protection.

Research subjects must receive an exact copy of any forms they sign or approve. One way to offer this is to photograph anything signed and send it to them, or have the research subject take a photograph.

2.2 Using "Consider data"

Ensuring data is protected and kept confidential is a wide-reaching obligation for researchers. Legal requirements in this area are defined by General Data Protection Regulations (GDPR), which specifically applies to personal data.

GDPR is described via many online sources, e.g., https://gdpr-info.eu. UCL advice on GDPR is here: https://www.ucl.ac.uk/legal-services/guidance/general-data-protection-regulation-gdpr/gdpr-essentials. The Information Commission Office's guide to GDPR is here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/. UCL offers online training.

STS expects researchers to understand the prescriptions of this law, and research will be stopped if these are not respected. STS **strongly recommends** those wishing to do small research projects, such as part of classwork, to design projects so the need to collect personal data is removed. Not collecting personal data in the first place creates **anonymous data**, which is free from GDPR requirements. Collecting personal data, then separating data and identifiers, creates **pseudonymous data**, which is ***not*** free from GDPR requirements (the key to linking identifiers and data must be protected as must the identifiers).

A. GDPR essential definitions

- personal data: any information relating to an identified or identifiable person (called the 'data subject') such as by reference to a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person;
- 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;
- 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;
- 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction,

In addition, STS researchers often gather **confidential information**. This is not a legal category. Its commonsense understanding relates to information a person might reasonably expect a researcher to treat as private or sensitive - something whose disclosure might cause embarrassment, awkwardness, or unwanted intrusion. An example would be a comment made about another person made during an interview. Or, financial information related to a business. Or, discussions covered under Chatham House rules. Or, material offered "off the record". Protection prevents both deliberate and inadvertent disclosure.

GDPR requires action should a problem with protection of data occur, or if a privacy breach occur. In STS, breaches normally must be reported to the STS Department Manager and to the project supervisor or line manager.

B. Protection of personal data

Data records are produced through data collection activities, such as interviews, surveys, questionnaires, searches of closed records (permission required), searches of open records (freely available), and so on.

Protection involves controlling access to data records, so no one can access information without your explicit permission. Your decision to permit access must be determined by the permissions agreed by the research participants and by GDPR. In digital settings, access can be difficult to restrict, but it is essential to prevent inadvertent leakage. Those considered to have access to digital assets include: (1) others with access to shared accounts, (2) suppliers of unencrypted cloud storage services, and (3) others with access to shared technologies, such as phones and tablets. Prior to application, researchers are encouraged to audit the access others have to their digital assets.

Controlling access normally takes the form of locks. Documents and artefacts can be stored in locked cabinets. Digital records can be password-access-only and stored in encrypted folders. It's not enough to keep physical records in a locked room, as lots of people besides you have access to the room. A locked box in a locked room is a standard solution. It's not enough to keep digital files on a computer that is closed by a single password. Personal data requires extra protection. Transfer of digital records must involve encryption and passwords. Disposal of records must respect privacy, too. Physical records can be shredded, burned, or disposed via confidential waste processes. Digital files can be disposed by data scrubber apps. Digital storage requires password-access and encryption systems. For instance, a USB pen drive easily can be lost, so it is a poor choice for storage, whether data is encrypted or not. Likewise, storage on a phone or transfer via email typically are insecure means for storage. UCL approves data storage on UCL managed servers, such as UCL Sharepoint, UCL Teams or UCL N: drives, and this is recommended in the first instance.

Privacy-by-design is a method for building privacy protections into our data collection processes, thus relieving us from some of the needs for later filtering or locks. On this method, if information is not needed, then it should not be collected. For instance, I should not ask for a declaration of gender unless this is a key variable in my methodology. Or, I should not ask for a name unless I intend to use it later, and if I need some code to identify participants, I simply use a random long number. Never collecting a person's name means I have saved myself one thing that needs protecting.

STS recommends anonymisation at the point of data collection as a preferred methodology for privacy-by-design unless special reasons apply. As a second choice, STS recommends immediate conversion to pseudonymous data records. Exceptional reasons should exist when avoiding anonymous and pseudonymous recording of data.

When processing data, sometimes data records are combined or shared. Sometimes information is extracted from data records, such as when information is transferred from questionnaires to spreadsheets, or from recordings to transcripts. When these continue to use personal data, those new compilations also are covered by GDPR. These must be properly stored. All processing also must have the specific opt-in consent of the research subjects.

Storage and disposal timelines should plan to keep original data until all reviews are complete, at the very least. For students, this may be the final exam boards associated with a module, or a viva. As a default, three months after the end of the degree programme normally is sufficient. For authors of publications, data must be preserved until after publication and peer scrutiny.

On accountability, STS expects researchers to be honest and forthcoming in their dealings over privacy. Breaches or difficulties must be reported immediately to supervisors or line managers, in the first instance, and the STS department manager, in the second instance.

2.3 Using "Consider safety"

Managing safety involves a mixture of common sense, anticipation, and planning. Supervisors and line managers are the first point-of-contact when discussing safety. You also can consult the STS Safety Officer. UCL offers training online and in-person for safety and risk management. Those considering a career in social sciences involving data collection and field work should avail themselves of formal training. RiskNet is the online tool for all UCL researchers.

UCL Safety Services is the supervening organisation for safety management and risk assessment < https://www.ucl.ac.uk/safety-services>.

A. lone working

One common activity in the work of STS researchers is working alone as an interviewer off-site from UCL premises and out-of-daytime working hours. This carries risks that need mitigation. For instance, interviewers should prefer to work in supervised spaces (e.g., cafes, open plan offices, or monitored meeting rooms) rather than private residences or behind lockable doors. They should know who is nearby who could raise an alarm if needed. They should leave details of itineraries with third parties, who will raise an alarm in the event of unexpected absence, and use pre-arranged check-in points.

Researchers working in public spaces or UCL spaces should identify people who might come to assistance (e.g., security guards, on-site emergency telephone numbers). Another mitigation can be to work in pairs or groups, or to work when accompanied by a friend or colleague.

STS has a "lone worker policy," which assists risk management.

B. travel to research sites

Another foreseeable risk involves travel to and from interviewing locations off-site from UCL premises. What's your entry and exit plan? A particular risk with travel involves getting stuck, such as when missing a train connection, or getting lost in route. Carrying numbers of reputable taxi firms, chosen in advance, can mitigate such risks (unless you think you might be out of phone or wifi range). Having pre-arranged plans for collection by car from a friend or relative in a "worst case" scenario offers another option.

C. digital privacy

Some researchers are comfortable mixing personal and professional contacts in email, Skype, telephone numbers, and so on. But some researchers are not, and they consider privacy as a potential risk. A common mitigation involves creating separate professional contact details, isolated from personal ones. Those working on UCL projects should use UCL-provided tools where possible. Staff can use auto-forwarding for telephone contacts.

D. equipment

STS research tends to involve recording equipment and portable digital tools. Risks often relate to robbery (thus putting people at risk of harm). Carrying too much can lead to injury. Setting up equipment can be non-trivial. Mitigation can involve keeping records and photographs of equipment carried into the field and ensuring UCL equipment is property tagged. It also involves plans for securing equipment when unattended. It also involves planning how cables, power supplies, stands, and such will be securely fashioned during use, such as to avoid trip hazards and obstructions to exits.

3. Top tips for STS researchers

Much research in our department involves minimum risk activities to collect non-personal data. Here are some top tips for speedy approvals. Discuss your plans with your supervisor or line manager as familiar solutions may be within easy reach.

A. methods

- prioritise minimum risk methods
- prioritise research questions that avoid "vulnerable groups" when timelines are short, as these applications require detailed consideration
- develop a one-page, plain-language information sheet that research subjects can keep; if collecting personal data, add a second page with specific information about data management and processing. Give the information sheet a serial number for easy reference (e.g., 2022-32). Pilot this on several independent colleagues before use in research.
- develop a one-page, plain-language consent form that presents positive opt-ins in a first-person voice (e.g., "I have read information sheet 2022-32. I consent to a recorded interview. I consent to …"). Use a serial number (e.g., 2022-ABC) for the consent form. Pilot it. Plan to leave a copy to the research subject.
- some methods will be referred automatically to UCL REC. If you think this likely, please ask the STS RRP lead.

B. data protection

- use privacy-by-design and collect no personal data (anonymous)
- when personal data is required, use pseudonymous methods by assigning each participant a long serial number as identifier, then storing the personal data in a password-access-only file that is stored solely on UCL central systems. Refer to individuals only by their identifier and non-specific descriptors, such as "interviewee 4662, who is undertaking a social sciences degree at a Russell Group university".
- treat consent forms as personal data
- do not store personal data of research subjects on your own laptop, phone, email system, or other open networks. Do not store personal data on cloud networks, USB pen drives, or other open portable devices. Use UCL networks in the first instance.
- do not use personal equipment for recording interviews or collecting personal data. Borrow STS equipment
- transfer interview recordings and digital records to secure, encrypted folders immediately after generating them. Have a system for recording the deletion of personal data from recorders, cameras, and other devices.
- store paper records and artefacts in the office of your supervisor or line manager if you do not have a locked cabinet of sufficient size or security. STS has secure storage for research materials.
- provide specific guidance on how a research subject might withdraw or request deletion of their personal data
- create a schedule for deletion of all personal data and name parties responsible for confirming these tasks

C. safety

- prefer methods that place you on UCL premises, or in open public spaces, during normal business hours
- if in a private or controlled space, work with colleagues or take a friend. As a second preference, research ways to raise an alarm, if necessary, and offer a plan for third-party knowledge of your itinerary.
- if travelling, offer two means for completing your route and return, such as given train schedules and phone numbers for taxi firms.

- if working digitally, consider separating personal and professional identities. If a postal address is required, STS can be used. Other tools can be arranged in consultation with your supervisor or line manager.