Research guidelines

Safeguarding and Complaints

Centre

https://centrethinktank.co.uk/

Date these procedures came into effect: 27/08/2026
Date these procedures must be updated by: 01/01/2027

This document sets out our research guidelines, what to do if you have a report of academic misconduct, what will happen if someone has made a report about you, and how reports are dealt with.

Who is covered by this policy? This policy applies to all members of Centre. This includes the Administration, Spokespeople, Regional/State Chairs, ex-members of Centre, and members of Centre Students. You can also make a report as a member of the public.

Part one

Purpose



Roles

- Researchers: To read these procedures and to keep up to date with them.
- The organisation: To enforce these procedures and provide training and guidance.

Aim of this policy

Individuals involved in research in any discipline for the think tank understand the set standards of expectation and educate or equip themselves to conduct research under the guidelines. The individuals show stewardship and create a research environment with integrity, supporting good research practice throughout the process.

Organisations that collaborate, advise, participate, co-create, and support research activity with Centre Think Tank will have policies and practices in place to create and support a good research environment. Organisations engaging with us will be aware and equipped to identify poor research practices and avoid or report this, rectifying or course-correcting as appropriate. They have transparent, robust procedures and ethical policies in place to recognise and have set measures to avoid malpractice, professional or academic misconduct.

Scope

The research guidelines apply to all individuals who undertake primary or secondary research for the think tank, represent, showcase, present, and collaborate on behalf of the think tank by physical presence, remote means, electronic platforms, or in hybrid throughout the period of engagement. It also applies to the events and projects where research is undertaken in any form with external bodies.

Preamble

The value, validity, and impact of all research rely on the integrity of the research. While the approach, organisation, and methodology of research and forms of output can be discipline or region-specific, the principles and professional codes that serve as the fundamental basis for the integrity of the research undertaken for any purpose. All research work in pursuit of advancement needs to be conducted with a sense of responsibility to research participants, end users, professionals, and the wider community through maintaining the highest standards of research ethics and integrity. The contribution to society through our research undertaking needs to be delivered through the core principles as outlined below.

Source materials

Our policies have been based on external procedures and agreements, including the 2011 managing and sharing data document published by the UK Data Archive, University of Essex, the 2016 UKRI Concordat on Open Research Data, the 2025 UKRI policy on the governance of good research practice, the Universities UK concordat to support research integrity, the 2021 Social Research Association Research Ethics Guidance, and the Social Policy Association Guidelines on Research Ethics.

Core Principles

Honesty in all aspects of research. This includes:

- Planning and gathering data
- Conducting surveys and study designs
- Reporting research methods and procedures
- Adhering to legal, ethical, and agreed means for sharing and releasing data
- Presentation of research goals, materials, results, and findings
- Acknowledging all entities involved and contributing to the research
- Making only justifiable claims from the research conducted.

Diligence and Excellence in Research Practice. This includes:

- Ensure scrupulous care and thoroughness from planning, delivery, to dissemination of research.
- Performing research adhering to the appropriate, agreed-upon methods and protocols.
- Being accountable for the credited aspect(s) and/or elements of the research work.
- Introspecting the validity of data before dissemination.
- Seeking approval from subject experts if the research involves matters outside your subject expertise.
- Open communications, including for research findings.

Show Respect and Care:

- To all the participants.
- Towards all samples, artefacts, and articles since they could be of cultural, historical, and personal value and irreplaceable.
- To mutually agree on processes that abide by good ethical practice.

Transparency. This includes:

- Declaring the aims and objectives
- Sharing with all participants at the earliest opportunity, how the data and information will be used.
- Declare conflicts of interest.
- Methods deployed in the study and specifics of materials, where applicable.
- Reporting negative outcomes where applicable.
- Publicising the findings of the research as appropriate, with the prior consent of all participants.

Part two

Definitions



Data: This can be information in oral, written, recorded, electronic, or a combination of these formats, collected or processed for the research.

Research data are the evidence collected or derived during a study to support, validate, or interpret research findings or formulate new theories. They can be quantitative or qualitative and come in various forms—digital, physical, or print. These include materials like statistics, interview transcripts, images, or observations, gathered through methods such as experiments, modelling, or fieldwork. Open research data is freely accessible and reusable with proper attribution.

Participants are members who engage in this action in any capacity.

Participation is defined as an action in the form of interviews, research work, observational studies, awareness campaigns, case investigations, collaborative work, and co-creation in oral, written, pictorial, and digital forms in person or remotely through telephone and digital platforms.

There are multiple forms of harm researchers should be aware of and should avoid:

- Psychological Harm: The emotional attachment that may form between researchers and vulnerable participants should be managed carefully. Provide support and relevant information when the research ends.
- Harm to Wider Groups: Be cautious about research findings that may unintentionally stigmatise or negatively portray certain groups. Avoid judgmental language in reports or publications.
- Researcher Well-being: Researchers should be aware of their own emotional responses when dealing with vulnerable participants. They should have systems in place for debriefing and seeking support when necessary.
- Physical Harm Procedures: Establish specific risk management policies for environments where physical harm could occur, including procedures for emergencies.

Part three

Data policy



This section includes the following subsections: data creation, processing, release, and storage.

- Data storage. The data collected, collated, and analysed need to be stored securely and released only as agreed at the start of the event with the stakeholders. Storage of data for a particular purpose, including length of storage, is set out in our Participant consent form.
- Processing: We operate a centralised model for data processing, managed by our team and, in most cases, our administration. We will also keep a consistent naming and structure for the data being stored.
- Encryption: This includes the use of strong passwords and encryption. On Windows, this includes 7-Zip, Veracrypt, or BitLocker. For Mac, the main service is FileVault, and on Linux, it is LUKS/dm-crypt.
- Security: Data will be stored on a secure and password-protected device. We also ensure that we only store the data needed for the project, for which we have permission.
- Sharing data: Data sharing must be secure and limited. For instance, using Nextcloud, Cryptpad, OnionShare, or another similar encrypted service for data sharing. Access will also be limited to the research team and only those who require access to the research. A spreadsheet inventory should also be created to track file names, contents, storage location, access permissions, and last modified or accessed.
- Secure backups: Backups must be stored on an encrypted USB drive. Where possible, we also use the 3,2,1 rule: 3 copies, 2 different media, 1 off-site, for instance, in the cloud.
- Artificial intelligence: AI will only be used for interviews where consent for this has been gained and where all of the contents of the interview, including any personal details, will be made public at the end of the research project anyway.

Data protection. Follow the Data Protection Act 1998, and all data will be processed following this. For cross-border data transfers, GDPR should be followed for EU countries, the Privacy Act 1988 for Australia, the Personal Information Protection Law in China, and other similar data protection laws. We also create a Data Management Plan for projects where necessary.

Citation. Any data which builds on the work of others must be properly cited and referenced by our authors. Data released by us should also be properly referenced when reused or cited.

Releasing data. All data from our projects is open by default. All data should be released using the FAIR (Findable, Accessible, Interoperable, Reusable) principles. The data will be released at most three months after the research is published, but we aim to do this immediately after. Data will then be available to the public indefinitely.

How we do this:

- All graphs, tables, and other data visualisations which were created using Flourish are set to allow anyone to duplicate the project and data. All of our data is released in this way or, for polling breakdowns, directly within our paper in a format which can be copied and pasted.
- Papers released on our website include dedicated data pages, which include links to the Flourish graphs which contain this open data and the interactive visualisations. All data released by Flourish uses an Open Data Commons Licence for all data we release.
- For data that can be stored in this way or cannot be released directly, it will instead be released using an alternative service. This includes services such as Zenodo.
- If requested using our info@centrethinktank.co.uk email address, we can also directly send any data using open formats such as CSV (tabular), FLAC (audio), TIFF (images), XML (qualitative). This is for raw data, videos, or audio files.
- To ensure data is open by default, all of our work is available to listen to or view on our website, YouTube, and downloadable using podcasting apps.
- All interviews which are not anonymous include a full transcript with speaker labels, which can be copied and pasted from our website.

Data dissemination: The collected data or the information shared by the participant in an activity can be shared upon informed consent. This data sharing or sharing identity, image in a specified activity must be communicated to the participants clearly at the earliest possible opportunity.

Reasons data may not be released: Our data will only be delayed or not released to protect confidentiality, if the data is from social media where our Head of Operations has decided the data is not really public such as where it is on a private forum, privacy or security, if it conflicts with the law or if anonymity is required to protect the confidentiality of the participant.

We will add a note to any work where data is not released, explaining the reasons why. For projects such as stakeholder mapping, data may be released after a time-limited period of exclusive first use.

Part four

Interview policy



At any stage

- If an individual withdraws consent, all data from the participant, any emails exchanged, transcripts created, video or audio recordings, and any other information should be deleted.

Preparation stage

- If the interviews are potentially of a very sensitive nature or a member of our team requests it, then a briefing session should be set up. This will be between the researchers, our Head of Operations, any specialists in the area, and any relevant Directors, and should be held for research of a more complex or very sensitive nature if required. This includes the emotional toll, additional safety precautions, cultural norms, interviews in dangerous areas, and for any to discuss any possible risks to confidentiality.
- Check the recruitment process for participants; do not invite young or vulnerable people unintentionally.
- Any incentives to participate in research or reimbursements should not interfere with benefits.
- Where possible, the participants selected for the study should be representative of the group being focused on or society as a whole, and the selection of participants is fair.
- The researcher creates an interview guide and open-ended questions. They check it through with fellow researchers, their manager, or in a mock interview.
- A consent form must be signed or consent given by another method which should be registered, and the records must be maintained. This can be adapted to socio-economic, cultural, and linguistic backgrounds. Participants in any study need to be clearly informed as to the purpose of the interview or study and the impact of such action. All participants need to provide informed consent. Informed consent means all participants understand what they are taking part in and what the aim and scope of that particular action. The implications of this participation, best understood at that point, should be made clear to the participants at the start of the engagement, and voluntary consent needs to be obtained. It is essential to ensure the participant is not coerced or unduly influenced in any manner and informed of the option of withdrawal from the study at any stage if they wish to do so.
- If the level of harm changes, then a new consent form should be signed.
- If possible, organise to interview with another individual, either another researcher or another team member. For in-person interviews, mobile phones should be carried if possible.
- Ensure to disclose any conflicts of interest.
- Pick a quiet, private setting for all interviews and ensure the location has appropriate accessibility when conducting in-person interviews.
- Assess whether the possible topics or planned questions in the interview will cause upset or distress. This can include topics such as trauma, abuse, or mental health. If so, this should be minimised as much as possible, and it should be clearly outlined to participants why these questions are relevant. Support resources should also be prepared, including sending participants the details of relevant helplines or websites that people can access.

- Assess the interviews to address any power imbalances, including whether individuals feel pressured to be involved. If you find an imbalance or are unsure, contact our Head of Operations using the contact details on our team page on our website.
- If working with vulnerable groups, follow our safeguarding procedures and follow the Mental Capacity Act 2005, which includes the assumption of capacity unless it can be proven otherwise.

Questioning and interviewing

- Ensure the person is in a safe location, especially during phone and online interviews.
- Ask open-ended questions and do not attempt to lead the interviewee down a particular path. This allows the participant to give a full, detailed, and free response. Do, however, steer them back to the topic in question if the conversation goes off on a tangent. The researcher can then ask follow-up questions to gain clarification.
- Check comfort throughout the interview. If participants become upset, the researcher should offer to reschedule or terminate the interview and should remind the participant that they can withdraw at any time.
- If the interviewee shows signs of distress or is becoming emotional, the researcher should offer to pause and allow them time to recover, reschedule, or terminate the interview, or they can withdraw at any time if they need to.

Post interview

- Email all participants a post-interview survey.
- After difficult or emotional interviews, team members may request a debriefing session or this may be set up by a Director or Head of Operations if this would be useful. This session would allow for emotional support and next steps to be discussed if further support is needed. This will be between the researchers, our Head of Operations, any specialists in the area, and any relevant Directors.
- A copy of the transcript, video, or audio recording can be provided prior to the release to the interviewee if requested by the individual or organisation.

Part five

Confidentiality policy



We have multiple procedures around confidentiality for participants in our research:

- Anonymisation should happen as early as possible.
- Raw data should be stored separately from identity links.
- Once an interview has been transcribed, anonymised, and checked, all copies of the recording should be destroyed. All identifying information will be destroyed within four weeks of the interview being concluded, once all of the information required has been collected from the individual.
- Remove personal identifiers (e.g., name, date of birth, address, National Insurance/NHS numbers) and instead use pseudonyms or participant numbers.
- Be mindful of indirect identifiers (e.g., job title, workplace, location, genetic data).
- Where verbatim quotes could expose the identity of a participant, instead use paraphrasing or refer to multiple cases at once.
- Ensure external organisations agree to confidentiality requirements, including transcribers, funders, subcontractors, and administrators.
- Avoid reporting small subgroup statistics that could indirectly reveal identities.

Part six

Limitation of methodologies policy



- Authors should explain details about methods, acknowledging limitations, and potential uncertainties.
- Report the findings of their research accurately and without trying to misrepresent results which do not align with the views of the author or preferred outcomes. This includes including outliers unless a good justification is included and dependent variables and conditions.
- For more complex methodologies, a quality assessment should be carried out by the researchers and then checked by our Head of Operations.
- Avoid overclaiming the validity of results based on unrepresentative samples.
- Ensure that verbatim quotes are presented with context and unique identifiers.
- Avoid selectively reporting results or misrepresenting findings.
- Ensure that all dependent variables and conditions are accurately reported, and p-values are not misleadingly rounded.
- Do not manipulate or cherry-pick statistical outcomes.
- If possible, work with a second researcher to evaluate the methodology and reduce bias.
- Ensure they avoid HARKing, or making a hypothesis after the results are known. The hypothesis must be written before data is analysed. In observational studies to synthesise evidence for informing policies, hypothesis driven is not possible but the study design needs to be carefully planned and checked before implementation. Even in observational studies, where researchers watch what is happening naturally and record the information, instead of doing experiments, used to gather evidence for policy decisions, you are unable to always start with a clear hypothesis, but it is still important to plan and review the study design carefully before starting.

Part seven

Process for breaches



Process for data, legal and ethical confidentiality breaches

- Lock down all systems and fully restrict access to systems.
- Notify the ICO if applicable.
- Inform participants about what happened, the type of data lost, any risks involved, mitigation measures, and steps they can take to protect themselves, such as resetting passwords.
- Fully investigate, including creating a timeline of the events, finding any affected data, a full list of decisions taken before and after, and recording all decisions and remediation steps taken.
- Find the solutions required to resolve the issue and make any updates to systems or additional training necessary.

Part eight

Research misconduct



It is important to be aware of the various forms we encounter in research misconduct.

Falsification
Creating false and/or inappropriate data of any nature, including composite media images, artefacts, and public information through manipulation. Making up or creating false data is an offence, and it is the responsibility of the participant to ensure the facts are established to the best of their knowledge.

Examples include:
- a) Data, which may be primary or secondary, obtained in this study or an analysis carried out on previously published, obtained data, should be presented in the form that is truthful and properly referenced.
- b) Falsification also includes misrecording people's views, thoughts,or opinions expressed in person, by phone, or on digital media. This can be from surveys, interviews, designed prospective, observational studies, market surveys, etc.
- c) Digital or physical manipulation of data, which can misrepresent the person, people, or information obtained at any given time, should be avoided at all times.

Plagiarism
Using, adapting, communicating, and publicising other people's ideas or work without their permission or citation. All work from any individual other than the author must be fully acknowledged.

Examples include:
- a) Using someone else's survey, interview, or other forms of data which were obtained for a different purpose and passing it as one's own work.
- b) Rewriting and adapting another person or organisations work for your own thesis, including paraphrasing. This also includes reports, journal publications, public presentations, press releases and other types of publication.
- c) Taking an idea and changing the words with the intention of passing this off as your own work.
- d) An author re-submitting the same piece of work multiple times whilst.

Fabrication
Making up any form of research output, including oral, written, art, craft artefacts, and digital matter that cannot be substantiated with evidence as original work by the researcher. This also includes creating false consents and communications.

Examples include:
- a) Creating, altering, and tweaking data obtained in any form to fit into one's hypothesis, the desired outcome, and polarised views will be data fabrication.
- b) Making up a number or data to show it carries statistical power, significance, and validity will be categorised as fabrication.
- c) Historical data, legacy information which may be unpublished, should not be misused.

Misuse of personal data
Personal data collected, collated or analysed in any form should be kept safely and securely. This cannot be revealed to others if informed consent is not obtained from concerned individuals or cohorts.

Examples include:

- a) Personal data obtained from patients or healthcare workers, for example, will contain sensitive data that should not be revealed without anonymisation.
- b) All data categorised as protected characteristics under the Data Protection Act should never be revealed to the public.
- c) Revealing personal or protected information to any other person, body or cohort which was not included in the original consent form when obtaining data from the concerned individual or body will be considered personal data misuse.

Inappropriate disclosure
The data or work that is in process or production should not be disclosed to others by mistake, gross negligence, or any form of manipulation at any stage. The disclosure of the outputs of the completed or incomplete work needs to be in line with ethical standards and good research integrity practice.

Examples include:

- a) Revealing any information to any other person, body, or cohort which was not included in the original consent form when obtaining data from the concerned individual or body will be categorised as inappropriate disclosure.
- b) A work undertaken for a body which results in data production should be disclosed to the commissioned or agreed bodies. This information should not be disclosed in any form to others before the completion or without the permission of the concerned individual or organisation.
- c) It will be inappropriate to disclose information in any form in channels and through means that are not agreed upon when undertaking the work.

Improper conduct
A participant involved in the research needs to meet ethical, legal and professional obligations at all times. Conduct with a lack of sensitivity to social and cultural backgrounds, with intent, would be classified as inappropriate.

Examples include:

- a) Undertaking any work, such as medical, scientific, social, and legal research, should first seek ethical clearance.
- b) All work that does not follow the ethical and professional framework in the respective disciplines can be considered improper conduct.
- c) Improper conduct may be perceived if the researcher does not act with cultural, social, and faith-based sensitivities during the research tasks, such as data collection, observational studies, interviews, and qualitative data work, for example.
- d) Misrepresenting data. For instance, “salami slicing” is where data is split into multiple publications, allowing for the data to be misrepresented.

Breach of duty of care
When conducting research, a duty of care is to be maintained throughout the study, and gross negligence, professional incompetence, deliberate or reckless action leading to harm would not be tolerated.

Examples include:
- All work should follow UK regulations at all times. Breach of duty of care comes into play when one has violated regulations under the Human Rights Act, research with vulnerable people, as directed and amended by the UK Home Office,

Improper publication and research output credits
Improper claim of qualification, competence, conduct of research, authorship, identity of participants, breach of confidentiality, misappropriation in the process of peer review, flawed interpretation, hiding relevant information pertinent to work, non-declaration of conflict of interest during the research, and at completion.

Examples include:
- a) All results must be shown, projected, and written out in line with the raw data and true observations of the result.
- b) Any attempt to physically, graphically, or digitally manipulate data in printed, published, or any form is research misconduct.
- c) All authors and co-creators must be given appropriate authorship. Our internal working procedures clearly set out the percentage of a publication that an individual must write to be given a particular title, such as an author, researcher, or editor, and we do not use ghost authors.
- d) All publications should be shown and circulated among all authors who are credited in the publication before it is sent out to publishers, released to the press or the internet.
- e) Other individuals or bodies who have helped generate this form of publication, including the entity bearing the publication costs, should be clearly acknowledged.

Be aware that the examples provided are not exhaustive. Manipulating data and inappropriate data handling, for example, can fall under more than one measure of Research Misconduct, including Data Fabrication, Data Falsification, Professional Misconduct, etc.

Part nine

Misinformation and disinformation



Definition
For this policy, misinformation is false or misleading information that is presented or shared as fact, especially when repeated, left uncorrected, or reasonably likely to cause or encourage significant public harm. Disinformation refers to the same, but with deliberate intent to mislead.

Examples of misinformation or disinformation sources
- Material from outlets formally identified by regulators, independent fact-checkers, or peer-reviewed research as consistently publishing demonstrably false claims. Any information from such sources must be clearly contextualised as originating from a source known to publish misinformation.
- Sources formally sanctioned by independent regulators.
- Court judgments or regulatory rulings identifying material as false or misleading.
- Claims that are presented as fact but are contradicted by multiple reliable sources, flagged as false, misleading, or untrue by independent fact-checkers, regulators, or peer-reviewed consensus.
- Unverified or misleading claims that clearly conflict with peer-reviewed consensus or trusted government statistical data.

Policy areas frequently targeted by misinformation and disinformation
- Climate change and global warming.
- 5G and radiation.
- Vaccination and public health.
- Specific groups, such as religious minorities and refugees.
- Elections and democratic processes.

Risks of using misinformation or disinformation
- Propagating false claims.
- Undermining the credibility of the research.
- Failing to meet obligations of reliability and validity.
- Misleading readers, policymakers, or other members.

Permitted use
Sources known for misinformation or disinformation may be used only when the purpose is to analyse or report on misinformation itself. For instance, in a study of misinformation narratives. Such material should never be treated as fact. A clear notice must accompany the work stating that the material is being analysed for research purposes and that the assertions are identified as false or misleading by sources recognised in the Hierarchy of misinformation detection, which can be found below.

Reasonable steps for detection

All information must be checked by the individual sharing the work, who must take reasonable steps to ensure accuracy and confirm that it does not constitute misinformation or disinformation. This includes verifying both the content and the reliability of the source. Researchers are required to use credible, verifiable sources, cite them correctly, and check all claims for accuracy.

- Confirm that the source has a reputation for accuracy and accountability (e.g. established scientific journals, statutory regulators, or IFCN-certified fact-checkers).
- Verifying assertions against multiple independent, reliable sources where available (e.g., peer-reviewed journals, regulatory rulings, or fact-checking bodies). This is particularly important for areas included in the "Policy areas frequently targeted by disinformation" list.
- If a claim cannot be fully verified, clearly label it as unverified either next to the source itself in the main body of text or at the top of the document if multiple sources are used. This should be confirmed with our main Director before publication.
- Document verification steps where this is reasonably practicable.

Hierarchy of misinformation detection

These are sources which are useful for detecting misinformation, and higher-level detection is often sources which have a purpose of detecting false information:

1. Independent fact-checking services. For instance, IFCN-certified fact-checkers such as Full Fact, as well as other established fact-checking teams that apply transparent methodologies, such as BBC Verify and Channel 4 News FactCheck.
2. Regulators, including The Office of Communications (Ofcom), fines for false news, Advertising Standards Authority adjudications, Medicines and Healthcare products Regulatory Agency, and Competition & Markets Authority.
3. Legal or regulatory rulings (Court judgments finding claims to be false or misleading, regulator adjudications).
4. Recognised bodies such as the Royal Society, the British Medical Association, the World Health Organisation (WHO), the Intergovernmental Panel on Climate Change (IPCC), and guidance from the NHS.
5. Academic or scientific evidence: peer-reviewed journals, systematic reviews or meta-analyses. For instance, Cochrane, The Lancet, or The British Medical Journal (BMJ).
6. Trusted knowledge bases such as ONS, Eurostat, the United Nations, OECD, World Bank, and IMF for economic/social claims.

Tests

An assertion will be treated as misinformation or disinformation if it meets two or more of the following four tests:

- Accuracy and Source Reliability: The claim is factually incorrect, distorted, omits essential context, uses misleading framing, or comes from a source with a recognised record of producing misinformation.
- Persistence and Repetition: The wider outlet or organisation has errors which are repeated, amplified, or left uncorrected, and move from being a one-off mistake into misinformation.

- Source Behaviour: The source ignores or rejects corrections, relies on unreliable evidence, or shows a pattern of distortion such as cherry-picking or repeatedly promotes information that has been debunked by independent fact-checkers.
- Harm and Impact: The information has the potential to cause or encourage public harm, including risks to health, safety, the environment, democratic processes, social cohesion, or the effective functioning of public policy.

The "assertions presented as fact" test
Centre Think Tank will not sanction members for holding protected beliefs or expressing opinions. This policy applies only to assertions presented as fact, including statements framed as discussion, hypothetical, conditional, exploratory, or part of academic debate, if the individual implicitly or explicitly suggests the assertion could be true. Disciplinary action applies where such assertions fall within the definition of misinformation or disinformation, regardless of the member's underlying beliefs. All assertions presented as fact must be verified and comply with this policy.

Examples of assertions presented as fact include:
- Quoting a source: A researcher references a statement from a news outlet known for disinformation. Even when quoted, the assertion must be verified and clearly labelled as misinformation if credible sources show it to be false or misleading. Failure to do so may result in disciplinary action.
- Academic debate framing: A seminar slide presents a discredited claim as a "contested topic." If reliable sources have demonstrated the claim to be false or misleading, it must be clearly labelled as misinformation, even when framed as debate. Failure to label appropriately may trigger disciplinary action.
- Hypothetical or conditional statements: A report states, "If these figures are correct, then X might happen." Even when framed conditionally, the underlying assertion must be verified and any uncertainty clearly labelled. Misleading or false assertions may lead to disciplinary action.
- Exploratory discussion: During a workshop, a team member suggests a controversial claim for consideration. If presented as potentially true, it must be verified and labelled as misinformation if unreliable. Failing to do so constitutes a breach of policy and may lead to disciplinary action.
- Public-facing commentary: A researcher tweets, "Some reports suggest X is happening," citing an unverified source. Even when tentative, the assertion must be verified and clearly qualified or labelled as misinformation. Sharing misleading claims may result in disciplinary action.
- Cross-organisation publications: A team member contributes to a report for another organisation, including an assertion from an unreliable source. All assertions must be verified and clearly labelled if misleading. Failure to comply may trigger disciplinary action.
- Media engagement: In an interview, a team member paraphrases a misleading or unverified claim. The assertion must be verified and clearly labelled as misinformation if unreliable. Not doing so could lead to disciplinary action.

- Historical or analytical framing: A researcher includes a false historical claim in a policy paper to illustrate a trend. Without labelling it as misinformation and verifying it against reliable sources, the claim is treated as an assertion subject to the policy. Non-compliance may result in disciplinary action.
- Inclusion of sources: Even if an individual writes in a team chat, "I personally have concerns about vaccines [links to a misinformation source], but I recognise that according to the scientific consensus, they are safe and effective," placing a source immediately after "I personally have concerns about vaccines" may lead readers to interpret the source as supporting that personal concern, effectively turning an opinion into a factual claim. Even though the second part cites the consensus, the juxtaposition creates ambiguity and could be treated as a misinformation risk. The inclusion of an unverified or misleading source in this context makes the statement an assertion of fact, and failure to verify and clearly label it may lead to disciplinary action.

Breaches of this policy include

- Using or sharing misinformation or disinformation within our organisation at any level unless it is a "Permitted use".
- Referencing outlets which have been repeatedly identified by regulators, independent fact-checkers, or peer-reviewed research as consistently publishing false claims.

Within Centre Think Tank

Sharing misinformation or disinformation within or connected to the organisation is prohibited. This covers all internal activities, including research, articles, drafts, interviews, events, team communications, social media posts and messages.

External sharing of misinformation

This policy also covers where team members share misinformation or disinformation external to their role. Our policy only applies to where the use of misinformation could reasonably be expected to cause reputational or operational harm to the Centre Think Tank. This does not require proof that harm occurred; only that harm was reasonably foreseeable given the member's role, and public association with the organisation such as: appearing on our team page. It includes the following:

- The individual sharing misinformation could undermine the reliability and rigour of the organisation's work, reducing its credibility given our commitment to high-quality and accurate research.
- Sharing or being linked to misinformation can erode confidence from stakeholders, including funders, partners, and audiences in the organisation's outputs, reducing credibility, willingness to collaborate, or provide support.
- Misinformation can reduce the impact of research, making it harder for policymakers and the public to rely on the organisation's findings.
- Think tanks rely on the public, policymakers, and institutions taking their research seriously. Misinformation can reduce influence and trust, making it harder to advance policy goals.
- Team members or members publicly linked to misinformation can damage relationships with other researchers, organisations, or professional networks.
- External perception of poor information practices can undermine staff confidence and adherence to research protocols, potentially lowering overall quality.

The use of “reasonable expectation” rather than actual, proven harm is employed as this takes into account the fact that in political or policy-focused organisations, most reputational harm is indirect and opaque. Funders, partners, or policymakers may act on perceptions without informing the organisation.

Some examples of how external sharing of misinformation may damage our reputation include:

- Funder relationship: A team member shares an unverified statistic on social media that is later shown to be false by ONS or a fact checker. Even if no funder ever communicates their concerns, it is reasonably foreseeable that a funder reviewing credibility could quietly reconsider or withdraw a funding request, or members may end their membership. This is true, especially as some donors may look to invest a large amount of money as a portion of their disposable income or a large sum of money.
- Policy credibility: A researcher publishes a policy paper (for Centre Think Tank or another organisation) that cites a debunked claim about climate change. Even if no policymaker directly complains, it is reasonably foreseeable that policymakers could treat the think tank’s outputs as less credible and adjust their engagement or reliance without informing us.
- Professional networks: A member reposts a conspiracy narrative about elections. Even if no collaborator objects, it is reasonably foreseeable that other researchers or partner organisations could quietly decide not to engage with us.
- External credibility spillover: A team member publishes misleading figures in work for another organisation. Even if no external party raises the issue, it is reasonably foreseeable that stakeholders, funders, or policymakers encountering that work could associate the errors with Centre Think Tank and downgrade trust in our research.
- Policy influence example: A researcher publishes an op-ed that repeats a false claim about vaccine side effects. Even if the outlet doesn’t issue a correction, it is reasonably foreseeable that health policymakers might view the think tank as unreliable, reducing their willingness to cite or meet with researchers.
- Media example: A team member tweets an unverified statistic about refugees from an organisation that regularly produces misinformation. Even without journalists raising it directly, it is reasonably foreseeable that media outlets could reduce invitations for commentary or stop citing the organisation’s research.
- Partner organisation example: A collaboration proposal is declined without explanation after another organisation notices that Centre Think Tank's work-cited material is already flagged as disinformation by a regulator.
- Public perception example: A misleading figure is included in a public-facing report. Even if stakeholders don’t raise it, it is reasonably foreseeable that reputational trackers, watchdogs, or informal networks could circulate the error, eroding public trust in the organisation’s reliability.

Factors in making a decision

- Sanctions will take into account intent, seriousness and repetition. Repeated sharing of misinformation means doing so more than once and can indicate negligence or disregard for policy.
- Honest mistakes, for instance, a single accidental inclusion of a source, will be treated proportionately and will often be used as a learning opportunity.
- Whether the individual followed the reasonable steps in the policy when sharing the assertions.
- Whether the source was clearly labelled as misinformation.
- The nature of the content shared.
- Whether the individual subsequently corrected the mistake.
- How the source was shared, for instance, knowingly, negligently, or as part of satire.
- When assessing potential breaches, decisions will take into account whether the source or claim is widespread or niche. Where fewer fact-checks or regulatory assessments exist, less external evidence may be required to reach a decision. In such cases, decisions will be based on the best available reliable sources as defined in the hierarchy of misinformation detection. Members remain responsible for exercising the reasonable steps required by this policy, even when limited sources are available.
- For information shared externally, determining whether the misinformation likely reached stakeholders, policymakers, media, or the public.
- For information shared externally, the individual's position or role within the organisation.
- Whether the individual made an “assertion presented as fact” as set out on the page below.
- Centre Think Tank reserves the final judgement, guided by the hierarchy of reliability, and any decisions must be documented with reference to these standards.

Part ten

Academic misconduct



Integrity and standards of research can be threatened or compromised by honest mistakes, errors or omissions. While it is imperative to follow best practices and avoid such errors through rigorous practice, it does not constitute research misconduct. Poor research practices such as inadequate background research, implementing techniques without personal, cultural or social sensitivity, misinterpreting data, poor record keeping, and poor research and implementation methods need to be addressed. This can be rectified through appropriate training to improve competency where needed and enhance practice through internal or external provisions. Honest errors or differences in research methodology are not considered misconduct.

The sections above outline both issues which may occur and practices to avoid. Any of these practices may be considered potential academic misconduct, which includes:

- Fabrication
- Falsification
- Plagiarism
- Failure to meet legal or ethical obligations
- Misrepresentation
- Violating our ethical framework
- Violating our data policy and misuse of personal data
- Violating our interview policy
- Violating our confidentiality policy
- Violating our limitation of methodologies policy
- Inappropriate disclosure
- Improper conduct
- Breach of duty of care
- Improper publication and research output credits
- Improper handling of allegations
- Misinformation and disinformation

Creating an environment where issues can be reported

- Non-Disclosure Agreements will and have never been used to prevent issues of academic misconduct from being raised or reported.

Preventing issues

We have a number of checks in place to prevent issues from occurring. Researchers must:

- Ensure they are clear and transparent about their methodologies and include a methodology section at the start of a publication.
- Carry out a risk assessment using the template within our safeguarding procedures to balance the risks and potential benefits of the research programmes. Ensure any harm to participants, wider groups and the public is also discussed more widely and addressed as far as practical.
- Have a duty to ensure that any issues they witness or are aware of are reported.

Each paper is reviewed by our Head of Operations to check for any breaches in our policies. They ensure:

- Participants, authors and stakeholders receive a copy of the paper before release.
- Any details of anonymous contributors are not included in the final version of the paper or transcripts.
- Check the ethical impact of the research, particularly on vulnerable and disadvantaged groups.
- The paper is checked for issues of bias, including whether conflicts of interest may not have been declared.
- Any falsification of research and misrepresentation of statistical analysis and research results. Any signs of this should be investigated thoroughly.
- Plagiarism checks using detection tools.
- That if, at any point in the research, they feel it is necessary, they may establish an ethics review board or ethical review processes with specialist members of our team and academic network. This can be used to evaluate high-risk or complex research, for complex issues arising during research or where these procedures may be broken.

During planning and before release, check for:

- Any suspected plagiarism, falsification or extreme bias should be reported under these procedures.

Training may also be given on:

- Ethical research
- Confidentiality principles.
- Working with vulnerable populations, including children, elderly individuals, and those with cognitive impairments.
- Data, including ethical recruitment practices, ensuring voluntary participation, access to data, guidance on indirect identifiers and anonymisation/confidentiality techniques, using sensitive data and consent strategies.
- Interviews include how to explain consent and participant rights, how to handle sensitive topics, manage distress during interviews, and provide emotional support.

Part eleven

Academic misconduct procedure



People. The Head of Operations oversees this procedure and they are the main contact for any issues, head up our academic data management work and are the main point of contact for ethics concerns. If an individual is not in post, the Director assumes responsibility for all of the roles set out in this document. Whilst they hold this post, they should act independently within the process; their investigation can also be followed up by the complaints team if the issue is serious. If the Head of Operations role is vacant at any point, then the Director will fill this role.

Sharing Information. Information about any suspected academic misconduct will be shared with the Head of Operations. This can include any of the information sent to us using the academic misconduct form; this is also listed in the "Methods to Make a Report" section of this document. None of these rules prevents any individual from discussing any details with the police, social services, or councillors for issues such as mental health.

When registering a report on our website, our form asks whether you agree to our sharing information policy. This means the person who made the report and the person the report has been made against should not share that a report has been launched, and they should not use identifying details whilst discussing the report. They should also not share any information given to them about the report that they did not know before the report was launched. A full explanation with examples can be found in our privacy policy. They can also share any information provided to them during the report to either the person making the report or the person being reported.

These last whilst the report is ongoing or until any police investigations are concluded. If any information is disclosed against our rules by either individual, then the Head of Complaints will need to sanction the individual, which can range from a warning to a suspension, depending on how serious the breach is. We will also inform the ICO if there is a data breach.

Dealing with allegations of research misconduct

Methods to make a report. Reports should be made through the academic misconduct form on our website in the complaints and safeguarding hub. This form can include your name, email address, whether you are a member, whether you have done anything to try and resolve the issue, the nature and details of the issue, including the names of those the report is about, if the report is an appeal, whether there is any additional evidence in the case, and the names of the people you would like to make a report about, how old they are, whether they are a member, and what region they live in, what position they hold, what you would like to see happen with your report, whether it is a joint report and whether you agree to our privacy policy.

Pastoral Support. Members or non-members may also get support from the Pastoral Care Officer during the process or more broadly during their time in Centre if they wish. This may be necessary if the person is under 18 or a vulnerable adult. This can include when submitting a report of academic misconduct, throughout the process, and after the process is complete, if requested.

Reports Against or By Former Members. If the person making the report, or the person the report is about, leaves Centre, then the report will still go through the system, and a report to the complaints team will still be made if necessary. This is to ensure members who have broken the rules in a serious manner are not allowed to remain within Centre. However, this means there will be no emails sent during the report process to former members if the report is against them.

Breaches of the Law. When a breach of the law is believed to be involved, then the issue will be reported to the police by the Head of Operations, the Head of Complaints or the Deputy Head of Complaints. If this happens, Centre will wait until the police investigation has been completed. If this takes more than six months, then we will follow up with the police to check when an internal investigation can take place.

This procedure can be used to report any suspected academic misconduct or harm caused by our research as outlined in our policies in the sections above. For researchers or those with knowledge of the research, including the general public, they can report an issue to the Head of Operations. Reports can be made to the Head of Operations by filling out the academic misconduct form. You may wish to include your name, or you may make a report anonymously.

Timeline for dealing with reports. The report should be dealt with in full, excluding any appeals, within three months of the report being made. Dealt with in full means either the case is passed on to our complaints team or a decision is taken. The Head of Operations dealing with the report must also keep the person who made the report up to date with any progress and, if the process overruns, they must explain why.

Email checks. To ensure emails are checked regularly by our Head of Operations, we confirm with this team member that they will carry out these checks and will inform us when they are no longer able to do so. We ask our Head of Operations to check the email once every four days. Our wider team can also check for any submissions on our website, although the only information received is the number of reports and when they were made. No personal information is accessible, and individual responses are not viewable. Our Head of Operations will then be notified once an email is received.

Acknowledging the report. When a report is received by the Head of Operations, they have four days in which to acknowledge that they have received the report. If you do not hear back from them within this time, you can email:

- Our Head of Complaints at complaints@centrethinktank.co.uk
- Our Deputy Head of Complaints at deputy.complaints@centrethinktank.co.uk
- Our Pastoral Care Officer at pastoral.care@centrethinktank.co.uk
- If you still do not receive a reply from any of the above, our main email address is info@centrethinktank.co.uk

Any communications should then take place only through the contact details provided by the person raising the issue or through the official email address for the Head of Operations.

They must then keep the person who made the report up to date with its progress, how it is likely to be dealt with, how long it will likely take, and if no further investigation will take place, why it is not something that will be investigated.

Informing the person that the report is against. The Head of Operations should request a copy of the latest membership data from the Director, the Deputy Director, or the Membership Officer. They should then email the person the report has been launched against to inform them within five days of receiving the report. This should also include the full details of the report that has been made.

Informing the Director that a case has been opened. At the beginning of the report process, the Head of Operations should send a small report to the Director stating the random number given to the report. At the start, it should simply say the rough nature of the report without any names or anything that could be used to identify the individual involved. They can also request the Director to suspend members of the team or Centre networks.

Anonymising the report. The Head of Operations then ensures that the information of the person making the report is anonymised. This will involve any details that may be used to identify the person, such as their name, gender, and age, being anonymised so any details that may be passed on to the complaints team will be purely about the case itself. To do this, each case will be assigned a number using Excel, and the people within the case will only be referred to as person A, person B, person C, and so on. The random number will be used for every email sent by the Head of Operations during the process. This process will be used for all cases, regardless of whether the person is remaining anonymous or not.

If you lose your email address during this process, then you should contact the Head of Operations with your report number to change future emails to that address with your case number.

Reports about members of our team. If a report is made against a member of our team, then they will not be allowed to take part in the process other than to give evidence.

If a member of the Administration, a Spokesperson, or a Regional/State Chair has a report made against them, then the Head of Operations should decide whether there is a case for them to suspend them from their position. This should take into account both the severity of the report and the likely outcome of the report. If the Head of Operations is the person the report is against, then the case should be immediately referred to the complaints team. When this person is suspended, the Head or Deputy Head of Complaints will need to send an email to inform them that they have been suspended from their position within five days of the original email informing them that a report had been made against them.

Investigating the report. When the investigation begins, the Head of Operations will email both the person who submitted the report and the person the report is against to inform them that the investigation has begun. It will be investigated regardless of whether the people involved are members or ex-members. Below is an outline of how decisions can be reached and what information should be compiled.

Initial investigation. The initial investigation will decide whether the case should go through the remaining procedure. The Head of Operations can ask for expertise from specific members of our team around particular research methods. A decision then needs to be made as to whether the issue requires further investigation. If it does not, then the individual who made the report and who was reported should be informed in the same way as if the process had been completed.

Gathering evidence. If a full investigation is to go ahead, then the Head of Operations should first gather evidence to help them decide on the case. This can include:

- Emailing those involved to better understand the case.
- Review any items of supporting evidence submitted throughout the process, such as documents or screenshots.
- What links, if any, exist between the individuals in the case?

Evidence must only be considered if it is:

- Relevant to the case and helps the person deciding on the report to reach a decision or understand the motivations involved. For instance, podcasts, TV episodes, and newspaper articles without direct links to the case itself are not usable evidence.
- Obtained through legal means. If there is any doubt about this, then the person providing the evidence can be asked about the background of the evidence during the investigation stage.

This should help the Head of Operations decide:

- What common facts can be agreed on in this case, where both the person who made the report and the person who is being reported about agree on them?
- What points of difference exist, what each person states happened, and where do these accounts differ?

Once the investigation is completed, both the person who made the report and the person the report was against should be informed that the investigation has concluded.

Deciding on the case

- Weighing up only the usable evidence available impartially.
- The standard for deciding a report is the balance of probabilities (the individual deciding the case needs to be satisfied that it is more than likely that the report is true).

To make this decision, the Head of Operations must decide:

- Whether they believe the allegation has been made in good faith.
- Those with allegations of academic misconduct against them must be informed and given a full explanation of the allegations. They must also have the chance to respond to the allegations in full.
- The formal investigation panel should consist of at least three members, with one from outside the organisation.

For cases where no evidence of misconduct is found, the individual the allegation is against and the person who raised the allegation must be informed.

Centre Think Tank will also protect the interests of the individual the allegations were against. This includes that if the allegation becomes public, then a public statement should also be released. This is alongside our policy to remove allegations which are malicious from the system, informing the individual of the case outcome, and individuals would have a right to appeal. Our rules must be in keeping with the Public Interest Disclosure Act 1998.

For cases of genuine oversight, the result may be discussing with the individual what good practice looks like or educating them. It can also be dealt with by the Head of Operations acting on their own or by the Director.

Malicious reports. Cases may also be passed on to our complaints team where the report itself is suspected to be malicious. This can be if an individual makes three or more reports that are not upheld. The Head of Operations can also reject reports if an individual makes two or more academic misconduct reports which are not upheld. This will be on an individual basis if the Head of Operations believes a specific report to be malicious.

The reasons a report itself may be considered malicious include:

- Abusive behaviour or language from the person making the report, verbally or in writing.
- The person making the report refuses to cooperate with the research guidelines procedure.
- The person making the report refuses to accept that the issue is not within our powers to change, investigate, or influence.
- Repeatedly insisting on seeing or speaking to a particular member of our team, which is not stated in the research guidelines procedure.
- Repeatedly demanding responses within an unreasonable timescale, for instance, within hours.
- Repeatedly breaching our code of conduct when making the report, for instance, through comments made during the process.

More widely, it should be assessed whether the report was submitted to:

- Create a disproportionate impact on the time and resources of volunteers who have to deal with them.
- Cause annoyance or disruption.

If a report meets these definitions, the complaints team will then write to the individual who made the report to explain why their report has been rejected. The individual who made the report can appeal this decision using the normal process for appealing complaints, but they may only do this once.

When considering whether a report is malicious, the complaints team should first take into account whether the cases previously submitted were difficult to decide on or whether they were clear-cut cases. They should also take into account whether the complaints were made purely to see a member suspended.

Suspected malpractice. Malpractice is usually where academic misconduct is intentional, repeated, serious in nature, or has serious consequences. If the Head of Operations deems a case to meet this threshold, they must pass the case on to the Head of Complaints. This must be alongside a report explaining why the case is considered to be suspected malpractice, who is involved, in what way, and the preferred response to the issue. The report will then be dealt with under our complaints procedure. This report must specify the nature of the issue, the overall findings of the report, and any evidence compiled as part of the investigation. Any funders or partners in the project must also be informed.

Genuine oversight. Once a case has been determined as a genuine oversight, suspected malpractice, or where there is no evidence, a report will be sent to the individual who made the original allegation, including why this decision was made and the supporting evidence.

Once an outcome has been decided. The Head of Operations will email both the person who submitted the report and the person the report was about. The other person's name should be anonymised if this is an anonymous report, explaining the outcome of the case, and outlining the next steps. This should also include a document explaining both the outcome of the report and the reasoning behind that outcome.

Informing the Director of the outcome. At the end of the process, the Director should be emailed to inform them that the case has been closed, and they need to be told what action needs to be taken, if any.

Learning lessons. These procedures will be reviewed if an incident occurs or if there is a ‘near miss’. To improve these measures, we may also talk to those involved in reports to ensure our practices are as effective as possible. This may include an action plan outlining steps the organisation as a whole can take and additional training required. Anonymised data on the allegations, outcomes, actions of any reports, how these issues will be avoided in future, any appeals, a note if no reports were made, and how long it took until these had been completed will also be added to our yearly reports. We will also keep anonymous records of all reports. This involves storing the information on a password-protected Excel document that only the Head or Deputy Head of Complaints can access. The records will be kept for four years, and after that date, they will be deleted.

Appeals process. If either the person who made the report or the person who was reported is unhappy with the outcome of the case, then an appeal can be made. The Head of Operations will then send an email to both the person who originally made the report and the person the report was against within one week to inform both that an appeal has been launched. They will also ask both individuals if there is any additional evidence they would like to submit.

The appeal will then be handed over to the Complaints team to make a final decision on who will be given anonymous details of the report, the original ruling, and any additional evidence submitted. The committee will decide whether to uphold the decision, to change the outcome put in place, or to overturn the decision. This process will mirror the process used for unclear complaints.

The appeal should be dealt with in full within three months. The original decision can only be appealed once, or when new evidence has been found that was not available before the original report was made.

Ensure these measures are kept up to date. These measures will be kept up to date to ensure our organisation can prevent mistakes from happening or learn from them if they do occur.

Availability of these measures. To ensure these measures are accessible to those who may need to consult them or go through the processes in this document, this document will be available on our website. A copy of this policy will also be sent to every member of Centre when it is updated by email.

Have any ideas to make these procedures better? Let us know by submitting any ideas on the “Contact” page of our website.

Centre

https://centrethinktank.co.uk/