Fact-Checking and Data Verification Policy in Scientific Center of Innovative Research

1. Purpose, scope, and relationship with other SCIR documents

1.1. This Policy sets out Scientific Center of Innovative Research (SCIR) principles and minimum requirements for fact-checking, data verification, source checking, and information quality control across SCIR activities, including publishing, projects, events, education, analytics, and public communications.

1.2. This Policy applies to materials and datasets that are created, used, processed, assessed, published, or disseminated through SCIR platforms and services, including journal workflows, conference outputs, project deliverables, educational materials, and public statements.

1.3. This Policy applies to authors, editors, reviewers, editorial board members, project leaders and team members, analysts, instructors, moderators, contractors, and any other persons involved in producing, validating, or approving information under SCIR.

1.4. This Policy operates alongside the SCIR Code of Ethics and Professional Conduct, the Artificial Intelligence Policy, the Complaints and Appeals Procedure, the Privacy Policy, and service specific rules.

1.5. The objective of the Policy is to protect the integrity of SCIR outputs, reduce the risk of errors, manipulation, and misinformation impacts, and ensure responsible handling of data, including data obtained through work with people.

2. External standards and documents informing this Policy

2.1. SCIR's approach to independent fact-checking and transparency is informed by the European Code of Standards for Independent Fact-Checking Organisations developed within the European Fact-Checking Standards Network (EFCSN).

2.2. SCIR's approach to procedural transparency and the correction of errors is additionally informed by the Arab Fact-Checkers Network (AFCN) Code of Principles and its open Correction Policy as a practical model for accountable correction practices.

2.3. Where relevant for cross-border comparability and good practice, SCIR also considers the International Fact-Checking Network (IFCN)

Code of Principles as a widely used benchmark for non-partisanship, methodology, and transparency commitments in fact-checking practice.

2.4. SCIR treats these external documents as methodological and ethical reference points. They do not replace SCIR's internal governance documents, but they shape how SCIR defines independence, transparency, correction practice, and evidence-based verification in its own operations.

3. Definitions

3.1. Fact-checking means the verification of claims against reliable evidence, including dates, figures, names, quotations, references, context, and logical consistency.

3.2. Data verification means procedures to assess the origin, integrity, correctness, completeness, and reproducibility of data, including validation of collection methods, cleaning, coding, aggregation, and analysis steps.

3.3. Primary source means an original source underpinning a claim, such as official statistics, legal acts, peer reviewed research, official organisational reports, or original datasets.

3.4. Secondary source means an interpretation or synthesis of primary sources, such as reviews, analytical articles, textbooks, or media publications.

3.5. Critical claims are claims that materially affect conclusions, recommendations, decisions, reputations, or may cause harm if inaccurate.

3.6. Project data means data collected, generated, accessed, or processed in SCIR projects, including surveys, interviews, focus groups, observations, administrative data, open data, experimental data, metadata, working tables, code, change logs, and outputs.

3.7. Human-derived data means any data obtained directly from participants or about participants, including personal data, biographical information, survey responses, interview materials, audio or video recordings, transcripts, task responses, test results, behavioural observations, and sensitive data where applicable and lawfully processed.

3.8. Data provenance means documented information about a dataset's source, acquisition, transformations, quality checks, versioning, and responsible persons.

4. Principles

4.1. Evidence priority. Primary and authoritative sources are required for critical claims and key figures.

4.2. Traceability and reproducibility. Claims and numbers should be traceable to sources and, where feasible, reproducible from documented data processing steps.

4.3. Transparency of method. SCIR expects clear description of how claims are selected for verification, how sources are assessed, and how conclusions are reached, consistent with EFCSN expectations on methodology and transparency.

4.4. Independence and non-partisanship. Verification work must be free from political or commercial interference and managed through conflict of interest safeguards, consistent with EFCSN and IFCN principles.

4.5. Human accountability. Tools, including AI, may support verification, but responsibility for accuracy, source integrity, and interpretation remains with the responsible human role under SCIR processes.

4.6. Harm minimisation for human-derived data. SCIR prioritises privacy, security, avoidance of stigmatisation, and mitigation of re-identification risk, especially for small samples or narrow groups.

4.7. Correction as accountability. SCIR treats timely and visible correction of substantive errors as a core quality requirement, aligned with AFCN's emphasis on open correction practice and EFCSN's transparency expectations.

5. Minimum fact-checking cycle for public outputs and project deliverables

5.1. Claim selection. Claims are prioritised for verification based on public interest, potential harm, reach, decision impact, and sensitivity of the topic.

5.2. Claim formulation. A claim must be stated precisely so that it can be verified against evidence.

5.3. Evidence collection. Verification requires identification and assessment of primary sources where possible, cross-checking key information, and recording limitations, time boundaries, and dataset versions.

5.4. Conclusion and uncertainty. Conclusions must separate verified facts from interpretation and clearly state uncertainty, assumptions, and constraints.

5.5. Documentation. For key numbers and conclusions, SCIR records core sources, dataset versions, transformations, and quality checks to support traceability.
5.6. Communication standard. Where SCIR publishes fact-checking outcomes or verification statements, it provides sufficient context to enable the reader to understand the reasoning, consistent with EFCSN transparency expectations.

6. Requirements for authors, analysts, and project teams
6.1. Authors and analysts must verify accuracy of numerical data, units, dates, names, organisational titles, legal references, and bibliographic details.
6.2. Quotations must match the original source. Fabricated quotations and non-existent references are prohibited.
6.3. Critical claims must be supported by primary sources or authoritative registries, with time coverage and version information where relevant.
6.4. Facts must be distinguished from opinions, assumptions, or forecasts, with clear labelling.
6.5. Project data must be documented through minimum data provenance elements, including source, access conditions, inclusion and exclusion rules, transformation steps, coding logic, and version control.
6.6. Where AI tools are used, the responsible person must apply enhanced checks for hallucinated references, misattribution, and statistical inaccuracies, and must comply with the SCIR AI Policy.
6.7. If a substantive error is identified after submission or publication, the responsible person must promptly inform SCIR and support correction, clarification, or withdrawal actions.

7. Requirements for reviewers, editors, and responsible coordinators
7.1. Reviewers assess whether conclusions are supported by the presented data and sources and flag obvious factual or methodological inconsistencies.
7.2. Reviewers are not expected to verify every fact, but must focus on critical claims, key figures, methodology, and source credibility indicators.
7.3. Editors and project leaders may apply risk based checks, request underlying tables, datasets, code, protocols, or logs, and initiate additional verification where risk is high.

7.4. Confidential materials, including manuscripts and human-derived data, must not be transferred to third party tools in ways that create confidentiality or privacy risks.

8. Special requirements for human-derived data

8.1. Before collecting or using human-derived data, the project defines the lawful basis, purpose, categories of data, sensitivity level, and data minimisation rationale.

8.2. Where informed consent applies, participants must be informed about purpose, data types, participation format, access rules, retention periods, and conditions for withdrawal, including how results may be published in aggregated or de-identified form.

8.3. For interviews, focus groups, audio, video, and transcripts, SCIR applies heightened confidentiality controls, including access restriction, secure storage, controlled copying, and controlled sharing within the team.

8.4. De-identification or pseudonymisation is a default safeguard where compatible with the project purpose. Re-identification risk is assessed, especially when datasets can be combined.

8.5. Public reporting based on human-derived data must avoid stigmatising generalisations and must use proportionate detail to prevent indirect identification.

8.6. If an error involves human-derived data or its interpretation, SCIR prioritises correction while minimising harm to participants and preventing further dissemination of harmful inaccuracies.

9. Corrections, clarifications, and withdrawals

9.1. Errors are classified as minor, substantive, or critical. Critical errors are those that change conclusions, key figures, recommendations, or may cause material harm.

9.2. Substantive and critical errors trigger corrective actions that may include visible corrections, clarifications, replacement of materials, methodological notes, or withdrawal or retraction where appropriate.

9.3. Corrections should be visible to the audience of the relevant resource, while internal records preserve an audit trail of changes, aligned with AFCN correction practice and EFCSN transparency expectations.

10. Training, monitoring, and policy review

10.1. SCIR maintains internal checklists and guidance for typical data types, including surveys, interviews, focus groups, open data, administrative data, ratings and indices, editorial analytics, and learning analytics.

10.2. This Policy is reviewed when legal requirements, donor requirements, technological risks, or relevant standards for independent fact-checking evolve, including updates to EFCSN, AFCN, or IFCN frameworks.

11. Contacts

11.1. Questions about verification requirements or reports of suspected inaccuracies, manipulation, or breaches should be submitted via SCIR official channels published on the relevant SCIR resource or subdomain.

References:

1. European Fact-Checking Standards Network (EFCSN). European Code of Standards for Independent Fact-Checking Organisations. https://efcsn.com/code-of-standards/
2. European Fact-Checking Standards Network (EFCSN). European Code of Standards for Independent Fact-Checking Organisations (PDF). https://static1.squarespace.com/static/5b20fe764611a08280b04412/t/63219bfc7c01cc10c04e0507/1663147007227/EU-CODE-EFCSN-.pdf
3. Arab Fact-Checkers Network (AFCN). Code of Principles (EN). https://arabfcn.net/wp-content/code-of-principles-en/
4. Arab Fact-Checkers Network (AFCN). Correction Policy. https://arabfcn.net/wp-content/code-of-principles-en/correction-policy/
5. International Fact-Checking Network (IFCN). Code of Principles. https://ifcncodeofprinciples.poynter.org/
6. European Digital Media Observatory (EDMO). European fact-checking organisations approve a Code of professional standards to combat misinformation (15 September 2022). https://edmo.eu/edmo-news/european-fact-checking-organisations-approve-a-code-of-professional-standards-to-combat-misinformation/

Annex A.
Operational Checklists for Fact-Checking and Data Verification

Public annex to the SCIR Fact-Checking and Data Verification Policy. These tables convert the Policy into repeatable controls for publishing, projects, analytics, education, and communications, including human-derived data.

Unified SCIR role glossary used in all tables

1. **Data Owner**: accountable for lawful access, provenance, permitted uses, and core field definitions.
2. **Data Steward**: accountable for data quality controls, access governance, versioning, change logs, de-identification, retention, and re-identification risk management.
3. **Data Analyst**: accountable for processing, QA checks, calculations, reproducibility, scripts, and transformation logs.
4. **Content Author**: accountable for factual accuracy in text, correct quotations, correct references, and clear claim framing.
5. **Responsible Editor**: accountable for risk based editorial verification, assigning additional checks, and decisions on corrections in the editorial workflow.
6. **Editor-in-Chief**: accountable for final decisions in high risk or disputed cases and for consistency of standards across services.
7. **Project Lead**: accountable for project governance, data management planning, ethical safeguards, and validation of project outputs.
8. **Communications Lead**: accountable for public news, press releases, rapid verification controls, and correction handling in communications.
9. **Platform Administrator**: accountable for technical access controls, security settings, logging, backups, publishing controls, and technical implementation of corrections.
10. **QA Reviewer**: accountable for independent second line checks for high risk outputs, indices, ratings, and high reach statements.

Table A0. Universal checklist for any SCIR public output

Control area	Verification questions	Evidence or artefact	Responsible role	Minimum level
Claim framing	Are all critical claims stated in a verifiable way?	List of critical claims	Content Author	Mandatory
Sources and primary evidence	Are key numbers supported by primary or authoritative sources?	Source pack with dates and versions	Content Author	Mandatory
Time validity	Is the data period aligned with conclusions and is an "as of" date stated?	Time window note, extraction date	Content Author	Mandatory
Numerical consistency	Do numbers match across text, tables, appendices, slides, dashboards?	Figure reconciliation log	Data Analyst	Mandatory
Context integrity	Are definitions, comparators, and context correct, with no selective framing?	Context check notes	Responsible Editor	Required for high risk outputs
Reproducibility	Can key indicators be reproduced from source data or intermediate tables?	Calculation file or code, transformation log	Data Analyst, Data Steward	Mandatory for indices, ratings, reports
AI related risks	If AI was used, were all facts, references, quotations, and attributions verified?	AI use note, verification record	Content Author	Mandatory when AI is used
Conflict of interest	Were COI disclosures collected and managed for key roles?	COI disclosures, decision note	Project Lead or Responsible Editor	Mandatory
Correction readiness	Is a correction route defined, including who approves and who publishes fixes?	Correction plan, contact	Communications Lead	Mandatory

Table A1. Survey data (human-derived)

Control area	Verification questions	Evidence or artefact	Responsible role	Minimum level
Instrument control	Are questionnaire, scales, and instructions archived with versioning?	Final instrument, codebook	Project Lead	Mandatory
Sampling logic	Are recruitment method, inclusion criteria, sample size, and limitations documented?	Sampling note	Project Lead	Mandatory
Fieldwork quality	Are duplicates, speeders, and abnormal response patterns checked?	QA log	Data Analyst	Mandatory
Data processing	Are cleaning, recoding, weighting, and exclusions documented and reproducible?	Script, transformation log	Data Analyst	Mandatory
Statistical integrity	Are base sizes, denominators, units, rounding, and ranges validated?	QA report	Data Analyst	Mandatory
Privacy and re-identification risk	Are de-identification controls and small group risks assessed and mitigated?	Risk note, suppression rules if used	Data Steward	Mandatory
Interpretation limits	Do conclusions stay within the methodological limits and uncertainty?	Review notes	Responsible Editor or QA Reviewer	Required for reports and recommendations

Table A2. Interviews, focus groups, audio/video, transcripts (human-derived)

Control area	Verification questions	Evidence or artefact	Responsible role	Minimum level
Lawful basis and consent	Is consent or other lawful basis documented, including recording consent where applicable?	Consent form, protocol note	Project Lead, Data Owner	Mandatory
Data minimisation	Are only necessary variables and identifiers collected?	Variable matrix	Data Steward	Mandatory
Confidentiality and access	Are access rights restricted and storage secured for recordings and transcripts?	Access register, storage controls	Data Steward, Platform Administrator	Mandatory
Transcription accuracy	Are transcripts validated through spot checks against recordings?	Transcript verification log	Data Analyst	Mandatory
De-identification	Are direct and indirect identifiers removed or pseudonymised where needed?	De-identified transcript version	Data Steward	Mandatory
Re-identification risk	Is re-identification risk assessed for small samples or rare attributes?	Risk assessment note	Project Lead	Mandatory
Quotation fidelity	Are quotations accurate and not taken out of context?	Quote-to-source map	Content Author, Responsible Editor	Mandatory
Harm minimisation	Does reporting avoid stigmatisation and unsafe granularity?	Ethical check record	Responsible Editor or QA Reviewer	Mandatory

Table A3. Open data and official registries

Control area	Verification questions	Evidence or artefact	Responsible role	Minimum level
Provenance	Is the publisher authoritative and clearly identified?	Dataset passport, publisher note	Data Analyst	Mandatory
Version and date control	Are version, release date, and extraction date recorded?	Version log, extraction record	Data Analyst	Mandatory
Licence and reuse	Is reuse permitted and are attribution conditions satisfied?	Licence summary	Data Owner, Project Lead	Mandatory
Coverage and limitations	Are definitions, coverage, and known constraints captured?	Limitations note	Data Analyst	Mandatory
Cross-checking	Are critical figures cross-validated by another authoritative source or logic checks?	Cross-check table	Data Analyst	Mandatory for critical claims
Transformation integrity	Are joins, filters, and aggregations documented and validated?	Transformation log	Data Analyst	Mandatory

Table A4. Administrative data and partner-provided data

Control area	Verification questions	Evidence or artefact	Responsible role	Minimum level
Access and legal basis	Are permissions, agreements, and processing terms documented?	Agreement, access approval	Data Owner, Project Lead	Mandatory
Data dictionary	Are fields, codes, units, and business rules defined?	Data dictionary	Data Owner	Mandatory
Quality checks	Are missingness, duplicates, anomalies, and time shifts tested?	QA report	Data Analyst	Mandatory
Comparability	Are definitions and measurement rules consistent across periods and sources?	Mapping table	Data Analyst	Mandatory
Partner influence boundary	Is it documented that partners cannot determine conclusions?	Governance note, process record	Project Lead	Mandatory
Output confidentiality	Are aggregation, suppression, and disclosure controls applied where needed?	Output control record	Data Steward	Mandatory when sensitive or human-derived

Table A5. Ratings, indices, dashboards, scoring models

Control area	Verification questions	Evidence or artefact	Responsible role	Minimum level
Methodology transparency	Are formulas, weights, normalisation, thresholds, and rules documented?	Methodology document	Data Analyst	Mandatory
Robustness and sensitivity	Are results tested for weight changes, missing data, and alternative specifications?	Sensitivity note	Data Analyst	Mandatory
Reproducibility by case	Can a score be reproduced for a selected entity end-to-end?	Replication file, run log	Data Analyst, Data Steward	Mandatory
Data provenance	Are source datasets, versions, transformations, and exclusions recorded?	Provenance pack, change log	Data Steward	Mandatory
Uncertainty communication	Are limitations and comparability boundaries stated clearly?	Publication notes	Responsible Editor	Mandatory
COI and independence	Are COI disclosures collected for designers, evaluators, and partners?	COI disclosures	Project Lead	Mandatory
Correction and versioning	Is a visible change log maintained and a correction workflow defined?	Version log, correction record	Communications Lead, Platform Administrator	Mandatory

Table A6. Journal editorial analytics (workflow and performance metrics)

Control area	Verification questions	Evidence or artefact	Responsible role	Minimum level
Metric provenance	Are source system, period, and extraction method stated?	Extraction note	Platform Administrator	Mandatory
Definition consistency	Are metrics defined consistently across journals and periods?	Metrics dictionary	Data Analyst	Mandatory
Anomaly detection	Are spikes and irregular patterns investigated and explained?	QA report	Data Analyst	Mandatory
Public claims validation	Are website statements reconciled with system records?	Reconciliation table	Responsible Editor, Editor-in-Chief	Mandatory
Change control	Are changes in counting rules documented to prevent misleading trends?	Change note, version log	Data Steward	Mandatory

Table A7. Learning analytics and education-related data

Control area	Verification questions	Evidence or artefact	Responsible role	Minimum level
Lawful basis and purpose	Is the purpose and lawful basis for analytics documented?	Process description	Project Lead	Mandatory
Data minimisation	Are only necessary fields collected, and can aggregation be used?	Field matrix	Data Steward	Mandatory
Access, confidentiality, retention	Are access rules and retention periods defined and enforced?	Access register, retention schedule	Platform Administrator, Data Steward	Mandatory
Data quality	Are missingness, duplicates, and logging gaps checked?	QA report	Data Analyst	Mandatory
Interpretation safeguards	Are conclusions contextualised to avoid misleading inferences?	Interpretation check notes	Responsible Editor	Mandatory
Harm prevention	Is profiling risk managed and is stigmatisation avoided?	Ethical check record	Project Lead, QA Reviewer	Mandatory

Table A8. Public news and press releases (high visibility communications)

Control area	Verification questions	Evidence or artefact	Responsible role	Minimum level
Claim inventory	Does the draft list factual claims and key numbers likely to be reused?	Claim inventory sheet	Content Author	Mandatory
Source threshold	Are critical claims supported by a primary source, or by two independent authoritative sources where primary is unavailable?	Source pack with dates and titles	Communications Lead	Mandatory
Dates and status accuracy	Are statuses correct, for example planned, announced, approved, launched, in progress?	Status verification note	Communications Lead	Mandatory
Names and affiliations	Are names, roles, and organisational titles verified?	Identity and affiliation check	Content Author	Mandatory
Quotations and permissions	Are quotations exact and properly attributed, with permission where required?	Quote approval record	Communications Lead	Mandatory
Numerical integrity	Are calculations, denominators, and rounding rules validated?	Figure reconciliation table	Data Analyst	Required for number-heavy releases
Legal, privacy, and harm risks	Does the release avoid personal data or sensitive details, especially from human-derived data?	Privacy and disclosure check	Data Steward, Project Lead	Mandatory
AI use and verification	If AI assisted drafting, were all facts and references independently verified and recorded?	AI use note, verification log	Content Author	Mandatory when AI is used

Control area	**Verification questions**	**Evidence or artefact**	**Responsible role**	**Minimum level**
COI disclosure	Where partners, funders, or evaluated entities are involved, are interests disclosed and influence boundaries stated?	COI statement draft	Project Lead	Required where applicable
Pre-publication sign-off	Is approval documented according to risk level?	Sign-off record	Responsible Editor or Editor-in-Chief	Mandatory
Correction readiness	Is a correction channel ready and is the correction format defined for the platform?	Correction plan, contact	Communications Lead, Platform Administrator	Mandatory

Annex A9.1. Standard Phrases for Preliminary Data and Subsequent Updates

Element	Content
Purpose	Provide consistent wording for posts containing preliminary data, updates, status changes, and uncertainty markers
When to use	Social media posts, short announcements, urgent messages, event notices, brief summaries
Channels	Any SCIR public channel where space is limited or publication tempo is high
Accountable roles	Communications Lead; for human-derived data also the Data Steward
Minimum control	Source threshold for critical claims, correct dates and statuses, readiness to publish updates

1) Preliminary information, verification in progress

1. “This is preliminary information. Verification is in progress; we will update once confirmed.”
2. “Data as of [date, time, time zone]. Updates may follow.”
3. “We are sharing preliminary results. Final figures will be published after verification.”
4. “Some elements are confirmed, others are being уточнюються. An update will be posted in this thread or as a separate message.”
5. “This is a working estimate based on currently available sources. Conclusions may change as new information becomes available.”

2) Status statements to avoid confusion

1. “Planned: [what], date: [date].”
2. “Announced by: [who], announcement date: [date].”
3. “Confirmed by: [who], as of: [date].”
4. “In progress: [step completed]; next step: [step]; expected date: [date].”
5. “Completed: [what], date: [date], outcome: [brief].”

3) Uncertainty wording that remains professional

1. “Sources differ on some details, so we are reporting only the confirmed elements.”
2. “The exact value is being clarified. The currently confirmed range is [X–Y].”
3. “We are publishing a conservative estimate; details will follow after data alignment.”
4. “There are data limitations: [brief]. This affects interpretation.”

4) Update wording

1. "Update [date, time]: source confirmation added; clarified [what]."
2. "Update [date, time]: replaced the preliminary figure [X] with the verified figure [Y]."
3. "Update [date, time]: status revised from 'announced' to 'confirmed'."
4. "Update [date, time]: corrected a description/name/title. We apologise for the inaccuracy."

Annex A9.2. Correction Notice Template for Social Media and Short Announcements

Element	Content
Purpose	Provide a uniform correction format so fixes are visible, clear, traceable, and do not create new risks
When to use	Substantive and critical errors; errors likely to be quoted; errors in figures, statuses, names, roles, affiliations
Channels	Social media, short announcements, news pages, partner channels where SCIR controls publication
Accountable roles	Communications Lead; when relevant Responsible Editor or Project Lead; for sensitive or human-derived data the Data Steward
Minimum control	Visibility of the correction; "was" and "correct" statements; basis for the correction; update trace; harm minimisation

1) General correction template

Heading: "Clarification", "Correction", or "Update"

Body:

1. "Our post dated [date] contained an inaccuracy."
2. "It stated: [briefly what was said]."
3. "Correct information: [correct information]."
4. "Basis: [primary source or brief description of verification]."
5. "We updated: [where the update was applied, e.g., 'in the post text' or 'in the attached file']."
6. "We apologise for the error and thank readers for their attention."

2) Correction template for figures

1. "Clarification regarding figures in our post dated [date]."
2. "It stated: [X]."
3. "Correct information: [Y], data period: [period], as of: [date]."
4. "Reason for change: [e.g., 'official dataset update' or 'denominator error identified']."
5. "Update applied in: [location]."

3) Correction template for names, roles, affiliations

1. "Clarification regarding a name/title in our post dated [date]."
2. "It stated: [incorrect]."
3. "Correct information: [correct]."
4. "The update has been applied. We apologise for the inaccuracy."

4) Correction template for statuses

1. “Clarification regarding the status of an item in our post dated [date].”
2. “It stated: [status].”
3. “Correct information: [status], as of [date].”
4. “This update is provided to avoid misinterpretation.”

5) Rules for corrections in short format (table)

Rule	How to apply	Accountable role	Minimum
Visibility	A correction must not be hidden; it must include “It stated” and “Correct information”	Communications Lead	Always
Update marker	If editing is possible, add “Updated [date, time]” at the start or end	Communications Lead	Always when possible
No editing available	If editing is not available, publish a separate correction linking to the original post or using a screenshot when needed	Communications Lead	Always
Cross-channel correction	For critical errors, repeat the correction in all channels where the original message was published	Communications Lead	For critical errors
Harm minimisation	If the error involves human-derived data, correct the substance without repeating sensitive details	Data Steward, Project Lead	For sensitive data
Audit trail	Keep an internal record of the correction, cause, verification sources, and update time	Data Steward or Platform Administrator	Always for substantive and critical errors

Annex A9.3. Triggers for Urgent Clarification or Correction in Social Media and Short Announcements

Element	Content
Purpose	Define clear signals indicating when a correction must be issued urgently, even if verification is ongoing
When to use	Social media posts, short announcements, news pages, partner reposts, fast moving notices and summaries
Channels	All SCIR public channels and partner channels where the message has spread or is likely to be quoted
Accountable roles	Communications Lead; for human-derived data also the Data Steward; for projects the Project Lead; for editorial materials the Responsible Editor
Minimum control	Avoid unnecessary repetition of the wrong claim while clearly correcting the substance and providing a contact channel

1) Trigger list for urgent correction

1.1. High reach triggers

1. The message has been picked up by partners, media, universities, donors, or is being widely reposted.
2. The post appears to be boosted, promoted, or has high engagement in a short time.
3. The message contains claims that are easily quoted without context, including figures, comparisons, rankings, or statuses.

1.2. Reputational harm triggers

1. The error may harm the reputation of a person, organisation, journal, partner, donor, or community.
2. The message implies misconduct, sanctions, violations, fraud, or conflicts of interest and this is inaccurate or unverified.
3. Names, roles, affiliations, authorship, peer review status, indexing status, or editorial decisions are stated incorrectly.

1.3. Legal and compliance triggers

1. There is a risk of defamation or unlawful statements about third parties.
2. Personal data has been disclosed or there is a risk of indirect identification, especially for small groups.
3. Copyright may be infringed, including images, graphics, or text used without appropriate rights.

1.4. Human-derived data triggers

1. Any error that may cause harm to research participants, stigmatisation, or safety risks.
2. Survey or interview findings are misreported in a way that changes meaning or context.
3. Details are published that were not covered by consent terms or that contradict data minimisation.

1.5. Factual integrity triggers

1. A claim is found to be unsupported by the primary source or was misinterpreted.
2. An error is found in denominator, units, percentages, rounding, time period, or comparison logic.
3. A break in series or methodology change is discovered that makes the comparison misleading.

1.6. AI related triggers

1. There is a suspicion that AI generated a fabricated reference, quotation, document title, or attribution.
2. The material was prepared quickly and did not undergo full manual verification of critical facts.
3. A mismatch between the text and the sources is identified, consistent with risks of automated summarisation.

2) Urgency levels and target response time

Level	Condition	Action	Minimum outcome
Level 1: Immediate	Human-derived data, privacy, legal risk, or reputational harm	Stop dissemination where possible; publish a correction or remove the post if channel rules allow	The error stops spreading and a visible clarification appears
Level 2: Urgent	High reach, key figures, statuses, indexing, partner statements	Publish a clarification and add "Updated"; prepare a full correction	Audience sees the correct fact and status
Level 3: Scheduled	Low risk, local inaccuracy without impact on conclusions	Correct in the next update cycle	The content is corrected without unnecessary amplification

3) Minimum urgent correction workflow

1. Identify which trigger applies and assign the urgency level.
2. Record what the error is and where it has spread.
3. Verify against the primary source or obtain an alternative authoritative confirmation.
4. Prepare the correction using Annex A9.2, minimising repetition of the incorrect claim.
5. Publish the correction in the original channel and, where needed, in all channels with reposts.
6. Save an internal record: cause, verification sources, time, accountable persons, and the publication reference.
7. If needed, prepare a brief note for partners to update their reposts.

4) Short partner notification template for urgent corrections

1. "We identified an inaccuracy in our post dated [date]. Please update or remove the repost."
2. "Correct information: [correct fact]."
3. "Updated version: [link or instruction where to find the update]."
4. "Thank you for your support, and we apologise for the inconvenience."