LEGAL DOCUMENT

Code of practice

Explains reporting, conduct, audience boundaries and review.

VERSION	0.6.0
REVISED (UTC)	2026-09-25 22:03:13 UTC
BODY SHA-256	bf913e830c5cc287295be68fa6471aa7a4416c4a78f0c0b294ffca350ab5574d
PUBLISHED AT	https://www.onsiren.com/legal/code/editions/0.6.0

This code sets the standards for factual safety reporting, proportionate sharing, review and respect for civil liberties.

01

Observe and describe

Report directly observed events, concrete behaviour, a relevant place and time, and the safety reason for sharing. Clearly distinguish facts, inference and hearsay. An earlier event may be relevant while a continuing specific risk exists; explain why.

Information not directly observed must be identified as such and its source made clear to the reviewer. The shared officer-report route follows the first-hand source rule. Authorised official notices use their separate route. Record the time of observation as well as submission.

02

Respect civil liberties

Peaceful protest, photography in public, a person's appearance or a protected characteristic do not by themselves establish wrongdoing. Reports must avoid discriminatory profiling and unnecessary disclosure of vulnerable people's information.

Use an identifying characteristic only where necessary for a specific lawful alert. Apply the same conduct-based criteria consistently, assess discriminatory effects and provide accessible challenge routes.

03

Use authorised source material

Do not upload shop CCTV, employer incident reports, customer records or internal workplace material to the shared network. A photograph you take still requires a necessary, proportionate purpose and an appropriate legal basis. Being outdoors does not remove privacy obligations.

The exclusion is the shared-network source rule. Separate business incident-reporting or future confidential employment casework requires its own collection and access design.

04

Review before disclosure

All alerts enter screening. Identifiable third-party material and allegations require human review before distribution. Human approval checks the basis, source, specificity, necessity, audience, retention and risk of harm. AI output alone is insufficient verification. Major events require independent corroboration and a clear confidence label.

Reviewers may seek information, reduce identifiers or audience, reject release or approve a time-limited alert. Keep account verification, report review and independent corroboration distinct. Any urgent provisional-warning route needs an expressly approved process. Routine workflow can use AI, with the existing team handling escalations; staffing numbers or new full-time posts are not specified by this code.

05

Keep the audience relevant

Apply approved place, role, purpose and time limits. No personal watchlists, intimidation, retaliation or further publication. A BID's member businesses have no automatic access through the BID's agreement.

Further disclosure requires its own lawful purpose and authorised route. A legally compulsory disclosure is assessed under the applicable obligation. Payment and membership do not expand the approved audience.

06

Correct and recall

Maintain a route to report errors, dispute identification and request removal. Record review outcomes and propagate corrections or withdrawal. Do not treat an allegation as a conviction.

Where the legal conditions apply, restrict disputed information while its accuracy is checked. Record the conclusion and notify recipients of required rectification, erasure or restriction unless impossible or disproportionate, with the exception documented. Any necessary retained dispute record must be clearly marked and access restricted.

07

Official notices

Official publishers must be verified for the purpose and jurisdiction. Missing-person appeals require an authorised source, a safety reason, minimal identifiers, a valid expiry and correction/withdrawal arrangements. Advisories may be general and contain no identifiable subject.

The publisher must confirm the notice's continuing authority and promptly report changed details or the end of its purpose. Assess children and vulnerable people individually and withdraw or correct the notice through the relevant channels. A missing-adult label alone does not establish a safeguarding condition.

08

Protect identities and private channels

Call signs reduce direct identification but remain linkable personal data. Ordinary moderators do not need reporter names. Group communications, official alerts, rights requests and union casework have separate access purposes.

Exceptional staff access to real identity must have a recorded purpose, authority and audit event. The current review model uses AI for routine administration, with the team administering and handling escalation; intended 24/7 human alert moderation remains to be evidenced.

09

Accountability

Human reviewers act under recorded responsibilities. Decisions, access, changes, complaints and holds need evidence. Compliance indicators identify specific checks and gaps. This centre's local checks do not establish the behaviour of unconnected production systems.

Before enabling the relevant production flow, complete the processing record, legal bases and conditions, DPIA, any required appropriate policy document, DPO assessment and breach-response arrangements. Each control records its owner, scope, evidence, review date and limitations.

10

Content reports and service safety

The final service must provide an accessible route to report suspected unlawful or harmful content and obtain the applicable review or complaint process. The public officer network and private group functions need a documented Online Safety Act scope assessment. If in scope, complete the applicable illegal-content risk, children's access and other required assessments and keep the controls and records current. Closed membership or an adult-user intention alone does not establish an exemption. Implementation and final service-safety rules remain to be verified.