



The Code of Conduct Action Kit

BY JANE
FRANKLAND MBE

THE IN SECURITY CODE OF CONDUCT ACTION KIT

A practical standard for respectful, inclusive and safer cybersecurity events — with a ready-to-use code, organiser guidance and clear badge terms.

Founded in 2017 by Jane Frankland MBE, the IN Security Movement developed its event code of conduct in response to reports of harassment and unacceptable behaviour at cybersecurity events. This edition retains that purpose while making expectations, reporting and organiser responsibilities clearer.

This is a model policy and implementation resource, not legal advice, certification or a guarantee of safety. Organisers remain responsible for adapting it to their jurisdiction, event and legal obligations.

How to use this kit

- Part 1 is a template: replace every [square-bracketed] field, publish it before registration and communicate it to everyone involved.
- Part 2 is the organiser implementation guide: appoint people, rehearse the response and prepare accessible reporting routes.
- Part 3 suggests wider actions to improve participation and inclusion.
- The IN Security commitment badge may be displayed only under the terms in Part 4.

PART 1 | EVENT CODE OF CONDUCT TEMPLATE

• Event: [EVENT NAME] • Organiser: [ORGANISER] • Dates and locations: [DETAILS] • Policy version: [DATE]

1. Our commitment

[ORGANISER] is committed to an environment in which everyone can learn, share, contribute and network without harassment, bullying, discrimination, intimidation or retaliation. We expect respectful conduct from everyone, irrespective of role, seniority, commercial influence or personal background.

2. Who and what this covers

This Code of Conduct applies to all attendees, speakers, sponsors, exhibitors, organisers, employees, contractors, volunteers, venue personnel and guests. It covers all in-person, virtual and hybrid events, including conferences, webinars, livestreams, online networking sessions and associated communities. It applies to event venues, online sessions, event apps, messaging platforms, social media, sponsor functions and event-associated social activities, including relevant communications and interactions before, during and after the event.

3. Expected conduct

- Treat others with courtesy, respect and professionalism, including when disagreeing.
- Respect personal boundaries, consent, accessibility needs and requests to stop an interaction.
- Follow reasonable directions from event staff and respect venue rules.
- Use photography, recordings, attendee data and event messaging tools responsibly and in line with stated permissions.
- Support someone experiencing misconduct without pressuring them to disclose details or confront anyone.

4. Unacceptable conduct

The following examples are prohibited. The list is not exhaustive:

- Sexual harassment, unwanted sexual attention, touching, suggestive comments or pressure.
- Discriminatory slurs, degrading remarks, threats, intimidation, bullying or persistent disruption.
- Stalking, following, intrusive contact or continued messaging after a person asks for it to stop.
- Inappropriate or non-consensual photography, recording or distribution of images or personal information.

- Harassment through event apps, direct messages, online meetings or social platforms; impersonation, doxxing and abusive manipulated or AI-generated content.
- Retaliation against someone who raises a concern, supports a report or participates in a fair review.
- Using professional status, sponsorship, employment power or access to opportunities to pressure or silence someone.

5. Report a concern

You do not need to confront the person involved. If you feel unsafe, move to a safe place and seek assistance. You may report conduct you experience or witness using any of these routes:

- In person: [DESIGNATED CONTACT / IDENTIFIABLE EVENT STAFF / LOCATION].
- Email: [DEDICATED REPORTING ADDRESS].
- Alternative or independent escalation: [SECOND CONTACT OR THIRD-PARTY ROUTE].
- Urgent danger: contact local emergency services and venue security: [DETAILS].

You may report anonymously, although limited information can restrict the steps available. You may share only what you feel able to share. Useful details, if known, include what happened, when and where, who was involved, any witnesses and immediate support needed. There is no requirement to provide a postal address or specify a desired sanction.

6. What happens after a report

We will prioritise immediate safety, listen respectfully, explain next steps and consider reasonable protective measures. We aim to acknowledge non-urgent reports within [e.g. TWO WORKING DAYS]; urgent reports will be assessed as soon as practicable. A designated person without a conflict of interest will assess the concern, seek relevant information where appropriate and determine proportionate action. We will provide updates where possible and tell the reporting person when the process has concluded, subject to privacy and fairness obligations.

Possible measures include separating individuals, changing access or schedules, warnings, removal from the event, exclusion from future events, sponsor or contractor action, and referral to relevant authorities where appropriate. Decisions are based on the available information and seriousness of the conduct. We will consider the wishes of the reporting person, but cannot promise any particular outcome.

7. Fairness, privacy and no retaliation

We will handle information discreetly and share it only with those who reasonably need it for safety, assessment, legal compliance or action. Absolute confidentiality cannot be promised. We will treat all involved fairly, manage conflicts of interest and prohibit

retaliation. Records will be retained and deleted under [ORGANISER PRIVACY NOTICE / RETENTION POLICY]. Reporting under this code does not restrict access to police, regulators, employment processes or other lawful remedies.

8. Accessibility and review

Accessible reporting options and reasonable adjustments are available on request: [CONTACT]. This code will be communicated before and during the event and reviewed after the event. Last reviewed: [DATE].

PART 2 | EVENT ORGANISER ACTION KIT

A. Before the event — implementation checklist

- Assign a named conduct lead and deputy; provide an independent escalation route for concerns about organisers, VIPs, sponsors or the conduct lead.
- Publish the completed code on the event website, registration journey, speaker/sponsor materials and event app; communicate it to contractors and venue staff.
- Ensure the reporting mailbox or channel is monitored during the event; provide at least one discreet in-person route.
- Train designated responders on listening, documentation, immediate safety, non-retaliation, fairness, confidentiality limits and escalation.
- Agree venue security, medical, safeguarding, accessibility and emergency arrangements as relevant.
- Define case ownership, response targets, records access and retention periods; seek legal advice for complex or jurisdiction-specific matters.
- Agree a graduated response plan and how decisions are made when sponsors, speakers or senior figures are involved.
- Check that photography, recording, event app messaging, virtual moderation and after-event activity are covered.
- For virtual and hybrid events: Provide an accessible, private reporting channel monitored throughout the event. Appoint a designated moderator or conduct responder with authority to intervene, disable chat or messaging functions, remove participants or restrict access where technically possible. Ensure participants know how to report concerns privately without having to raise them publicly.

B. When a concern is raised — response sequence

1. Protect

Check immediate safety and wellbeing; summon emergency assistance if necessary. Avoid forcing confrontation or mediation.

2. Listen	Receive the account without blame, pressure or promises of secrecy. Ask what immediate support is needed.
3. Record	Record necessary facts securely and accurately, distinguishing observations from allegations and conclusions.
4. Assess	Assign an impartial lead, consider conflicts of interest and assess risk and proportionate interim measures.
5. Decide	Seek relevant accounts fairly; determine appropriate action and escalation. Preserve evidence lawfully.
6. Follow through	Communicate appropriate updates, monitor retaliation risk, document closure and identify preventive improvements.

C. Example reporting form — optional fields

Event/date: []

Preferred contact method: []

Anonymous report: [YES / NO]

What happened, where and when (if known): []

People involved and witnesses (if known): []

Is anyone currently at risk or in need of support? []

Relevant evidence or links (optional): []

Preferred communication/accessibility adjustments (optional): []

Privacy note: explain who receives the report, why data is collected, how long it is retained and any required disclosures. Do not request unnecessary sensitive information.

D. After the event — evidence of implementation

Prevention	Were staff briefed? Were reporting routes visible? Were accessibility needs considered?
Response	Were reports acknowledged and triaged promptly? Were conflicts managed and protective steps taken?

Confidence	Did participants know how to report? Did they trust the process? Would they feel comfortable returning?
Learning	What recurring risks, gaps or improvements were identified? What will change next time?

Review trends using aggregated, privacy-conscious information. A low report count does not necessarily mean an event was safe; it may indicate a lack of trust or awareness. Avoid publishing details that could identify people.

PART 3 | BUILDING A MORE INCLUSIVE CYBERSECURITY INDUSTRY

The IN Security Code of Conduct was created to address unacceptable behaviour and make cybersecurity events safer, particularly for women who had reported harassment. That mission remains important. Inclusion also requires action beyond an event policy.

Actions for organisers

- Build diverse speaker pipelines through open calls, outreach, mentoring and fair selection criteria; review representation without reducing inclusion to one target.
- Design accessible formats, fair speaker arrangements and welcoming networking opportunities.
- Ask sponsors and suppliers to uphold the same behavioural expectations.
- Gather feedback on participation, psychological safety, reporting confidence and barriers to attendance.

Actions for speakers, sponsors and attendees

- Model respectful behaviour and intervene safely as a bystander, for example by seeking staff help or supporting someone who wishes to report.
- Challenge exclusionary assumptions and help amplify qualified voices that are less often heard.
- Offer introductions, sponsorship, mentoring and speaking opportunities without demanding unpaid labour.
- Treat colleagues fairly in meetings, hiring, promotion and professional recognition.

Remember why this started

The Code of Conduct began in 2018. In the Movement's 2019 research involving 2,157 women, 26% reported experiencing sexual harassment at a cybersecurity conference and at least 40% reported experiencing discriminatory or otherwise inappropriate

language or behaviour. These are historical research findings, not current prevalence estimates.

PART 4 | IN SECURITY COMMITMENT BADGE: TERMS OF USE

What the badge means

The badge signifies that an event organiser has publicly committed to adopting and implementing the IN Security Code of Conduct. It is a declaration made by the organiser, not an independent verification, certification, accreditation, endorsement or guarantee of an incident-free event.

Conditions for free use

- The organiser must publish an accessible event-specific code that meets or exceeds the substantive expectations in Part 1, including reporting, non-retaliation, impartial assessment and enforcement.
- The organiser must identify usable reporting contacts, appoint responsible people and take reasonable steps to implement the policy in practice.
- The organiser must communicate the code to attendees, speakers, sponsors, staff and relevant contractors before or at the event.
- The badge must be accompanied by a link to the event's published code and the statement: "We have adopted the IN Security Code of Conduct and commit to implementing it at this event."
- The organiser must not imply that IN Security or Jane Frankland has inspected, approved, audited, certified, sponsored or endorsed the event.
- The badge artwork must not be altered, combined with another mark in a misleading way or used for unrelated products or general corporate certification.
- Use is free, non-exclusive and revocable. The IN Security Movement may request removal where use is misleading, conditions are not met or the badge brings the initiative into disrepute.
- Permission applies only to the authorised IN Security commitment badge artwork supplied for this purpose; no broader rights to the IN Security name or logos are granted.

Suggested public disclosure alongside the badge

"Our event has adopted the IN Security Code of Conduct. We commit to respectful conduct, accessible reporting, fair assessment of concerns and proportionate action where needed. The IN Security badge represents our public commitment; it is not an independent certification or endorsement."

How to adopt

1. Download this free kit.
2. Complete and publish the event code.
3. Assign and brief responsible staff.
4. Make reporting accessible.
5. Display the approved commitment badge with the required link and statement.
6. Review implementation after the event.

Organisers may adapt the template to local requirements and strengthen protections. They should not remove essential reporting, anti-retaliation or enforcement provisions while claiming adherence. Attribution: “Based on the IN Security Code of Conduct, founded by the IN Security Movement (2018).”

PART 5 | LIABILITY, RESPONSIBILITIES AND DISCLAIMER

These terms apply to the IN Security Code of Conduct template, accompanying Action Kit and permission to display the IN Security commitment badge. They are separate from the event-specific code that an organiser publishes for participants.

1. Publisher and purpose

The IN Security Movement is an initiative associated with Jane Frankland MBE and KnewStart Limited. This resource is made available free of charge as general guidance to help event organisers create respectful, inclusive and safer events. It does not constitute legal, regulatory, safeguarding or professional advice.

2. Organiser responsibility

Each organiser is responsible for deciding whether the template is suitable for its event and jurisdiction; adapting and publishing its own policy; training staff; providing accessible reporting routes; handling complaints fairly and lawfully; safeguarding participants; and complying with applicable laws. Adoption does not transfer event management, incident-response or participant-safety responsibilities to the IN Security Movement, Jane Frankland or KnewStart Limited.

3. No certification or safety guarantee

Display of the IN Security commitment badge records the organiser’s public commitment to implementation. It is not an audit, accreditation, certification, independent verification, sponsorship, endorsement or approval by the IN Security Movement, Jane Frankland MBE or KnewStart Limited. Neither the code nor the badge

guarantees that harassment, discrimination, misconduct or other incidents will not occur.

4. Limitation of liability

To the fullest extent permitted by applicable law, the IN Security Movement, Jane Frankland MBE and KnewStart Limited exclude liability for losses, damages, claims, costs or expenses arising from an organiser's use, adaptation, implementation or non-implementation of this resource; its enforcement decisions; or the conduct of event participants or third parties. Nothing in these terms excludes or restricts liability that cannot lawfully be excluded or restricted, including liability for death or personal injury caused by negligence, fraud or fraudulent misrepresentation.

5. Free permission and conditions of use

Organisers may reproduce and adapt the event code template for their own events without charge, provided they do not falsely claim endorsement or certification by IN Security. Permission to display the official badge is separate, conditional, non-exclusive, non-transferable and revocable, and is governed by Part 4. The badge and IN Security name may not be modified or used to suggest wider endorsement. All rights not expressly granted are reserved.

6. Withdrawal and misleading use

KnewStart Limited, as publisher of this resource, may request correction or removal of the badge where an organiser misrepresents its meaning, does not meet the published conditions, or uses it misleadingly. The publisher is not obliged to monitor, investigate or verify every adopting event. Withdrawal of badge permission does not replace any organiser duty to respond to concerns or comply with the law.

7. Privacy and legal compliance

Organisers are responsible for providing their own privacy information and handling incident reports and personal data under applicable data protection laws. They should obtain independent legal advice where needed, especially for international events, employment-related complaints, safeguarding concerns and the legal enforceability of their own event terms.

8. Acceptance of terms

By using the official IN Security commitment badge, an organiser agrees to the conditions in Parts 4 and 5. If the badge is distributed through an online registration or download process, the publisher should require an affirmative acceptance of these terms and retain a record of the version accepted. Merely downloading the freely available template does not imply that the organiser has been assessed or approved.



About the IN Security Movement

The IN Security movement has been going since 2017. From one book, which Jane Frankland MBE wrote, to a global force for inclusion, access, and cyber resilience.

We're on a mission to create a safer, more equitable digital world – by removing barriers and unlocking access for the brilliant minds too often overlooked.

Whether you're a woman trying to break into cyber, a young entrepreneur building something new, or part of a community that's long been excluded, you deserve access to tools, insights, and opportunity. And that's exactly what we're here to give.

Partner with Us

To work with us as an active partner, email our founder, Jane, at: hello@jane-frankland.com.

Join the IN Security movement

Join the IN Security movement:
<https://bit.ly/INSecurityMovement>

About Jane Frankland MBE

About Jane Frankland MBE
Jane Frankland MBE is an author, strategist and authority on cyber survivability. With almost three decades of experience in cybersecurity, she is known for her work on leadership, culture, accountability and inclusion. She founded the IN Security Movement and has supported hundreds of women through cybersecurity scholarship opportunities.