skillcast

Moving from Policy to Proof

ERA 2025 E-book

Under the Employment Rights Act (ERA) 2025, harassment prevention is moving from policy statements to systems that can stand up in court and with regulators. The bar is “all reasonable steps” are evidenced through end to end controls.

The essentials are known: a plain English policy with examples, multiple reporting routes, including an anonymous route, defined triage and investigation playbooks with timelines, non retaliation safeguards and calibrated outcomes.

The differentiator is execution at scale: coverage, consistency, and learning across the incident lifecycle.

Building the evidence

Moving towards placing proof ahead of policy requires:

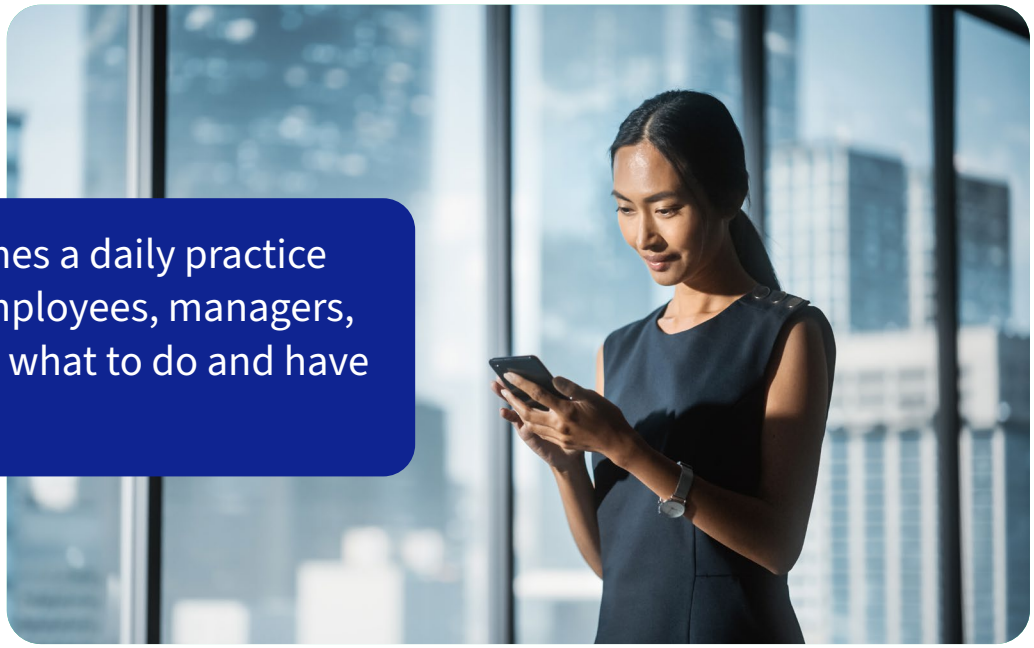
- Role specific training
- Operational monitoring
- A single source of truth for cases and metrics

It also means a **proactive stance on culture**, because microaggressions, banter, and blurred boundaries often precede misconduct.

Expectations should be explicit, modelled by leaders, and enforced in practice, especially in high contact environments where risks extend to customers, suppliers, and other third parties.

1. Build an integrated framework that links policy, training, contracts, and operational controls to measurable outcomes.
2. Map roles with public or client exposure, zone high risk environments, and design for safety with lone working protocols, visibility, and rapid support.
3. Codify norms for on site and online behaviour, set expectations for client entertainment and alcohol, and brief client facing teams on conduct clauses, refusal of service authority, and escalation protocols.

Prevention becomes a daily practice when frontline employees, managers, and leaders know what to do and have the tools to do it.



Building a risk management process

It is important to treat behaviour risk like any other business risk: define metrics, instrument the process, and close feedback loops.

Ensure your business has measures in place to minimise this risk:

- **Track training completion and assessment performance** by objective, monitor reporting volumes and time to resolution, and analyse helpline themes to spot demand and bottlenecks.
- **Provide multiple confidential reporting routes** with visible anti-retaliation safeguards, and publish what to expect when reporting to build trust.
- **Maintain secure, auditable records** spanning policy changes, training cohorts, assessments, communications, and remedial actions.
- **Map risks** across customer facing roles, high pressure teams, social events, night shifts, and field operations, with documented mitigations such as supervision, alcohol controls, client conduct clauses, and staffing patterns.
- **Update contracts, NDAs, and settlements** to avoid silencing whistleblowers or discouraging reports, and validate reality with audits that pair pulse surveys with qualitative interviews to confirm practice matches policy.

Building a defensible anti-harassment system

Effective training is segmented, measurable, and recurring.

Managers need different content than individual contributors; people partners and leaders need deeper modules on triage, escalation, sanctions, and retaliation risks

Apart from the steps outlined to minimise risk, a defensible anti-harassment system requires alignment of procurement and client management with contractual rights to act when third parties harass staff, including withdrawal mechanisms and escalation triggers.

Culture plays a big role in building a solid system. Shape culture with deliberate scripts for early interventions and scenarios that translate values into clear expectations and consequences. Speak-up systems are governance assets. Whistleblowing protections must also explicitly cover sexual harassment disclosures across past, present, and likely incidents.

There should be separate intake for grievances, whistleblowing, and safeguarding to set the right process and duty of care. Use competent, independent investigators to avoid conflicts and preserve trust; treat confidentiality boundaries, defensible notes, proportionality, and timeliness as non-negotiable.

Oversight is vital. Run operational retaliation monitoring: track work allocation, ratings, shifts, assignments, and social exclusion indicators; intervene when patterns signal backlash.

Maintain a central case register capturing:

- Allegation type
- Business area
- Seniority
- Protected characteristics
- Time-to-triage
- Time-to-resolution
- Outcomes
- Remedial actions

Use the dataset to build board dashboards, evidence "all reasonable steps," target training and manager coaching, and refine risk controls such as limits on one-to-one client entertainment or chaperoning in high-risk contexts.

Building protection that is provable

Execution turns standards into protection. This process is critical for employers under the ERA 2025.

1. **Start with a gap analysis** across policy, training, reporting channels, investigation capability, retaliation safeguards, and sanctions against higher duties and day-one rights.
2. **Convert gaps into a prioritised roadmap** with owners, milestones, and KPIs: training coverage and timeliness, time-to-triage, case age distribution, substantiation and outcome calibration rates, and post-case retaliation metrics.
3. **Upgrade probation frameworks** before the six-month dismissal threshold: define objective criteria, schedule mid-probation reviews, implement support plans, and standardise extension templates.
4. **Elevate manager capability** with short, scenario-based modules on reasonable adjustments, family leave conversations, performance feedback, and early conduct interventions.
5. **Standardise documentation**, including contemporaneous notes, decision rationales, outcome letters, to reduce disputes and build defensible cases.
6. **Stress-test high-risk contexts** through tabletop exercises; embed independent escalation paths via HR, legal, and safeguarding; enable bypass of line managers when conflicts exist.
7. **Use pulse surveys** to measure psychological safety and reporting confidence, then triangulate with case data to identify silent hotspots.
8. **Tie risk to reward** by linking leadership incentives to conduct and safety metrics.

It is important to have an accessible policy that you can embed into onboarding, performance management, and supplier and client contracts. Map end-to-end concern handling: intake, triage, confidentiality limits, escalation, investigation, feedback to the reporter, and remediation tracking.

Manage third-party risk through contract clauses, clear consequence frameworks, and escalation ladders aligned with client and supplier governance. The goal is a system that detects early, investigates fairly, protects reporters, and proves that nothing material was missed.

Training must operate as an evidenced control, not a checkbox. Build differentiated tracks aligned to decision rights and responsibilities.

- **For all employees,** cover definitions, realistic examples (including “banter,” invasive comments, exclusion, unwanted attention), bystander options, and reporting choices; make it explicit that intent is irrelevant and a single event can be unlawful if it creates a hostile or degrading environment.
- **For managers,** add intake scripts, non-retaliation reminders, documentation standards, immediate safeguarding steps, and how to handle low-evidence allegations or misconduct by high performers.
- **For senior leaders,** focus on oversight duties, resourcing, consequence management, and how to audit for effectiveness.

Prove comprehension through scenario-based assessments, track completion and refresh cycles, and pulse-check sentiment post-training. Integrate attendance, results, reminders, and remedial coaching into HRIS and case management tools to convert training into a controlled operational capability that can withstand regulatory and stakeholder scrutiny.

Building a safer workplace

Use contracts as a force multiplier. To ensure you have a safe working environment, you need to build conduct clauses, incident logging obligations, and defined consequences into client and supplier agreements to align partners with your standards. Give teams clear authority to refuse service and to call in supervisors without penalty.

Tighten confidentiality practices:

- Avoid provisions that restrict allegations or lawful disclosures
- Update settlement templates and employment contracts with carve outs for whistleblowing, regulators, and medical or therapeutic professionals
- Require independent legal advice
- Consider cooling off periods

Even though policies are no longer enough, it is important to keep them as well as templates up to date with changing statutes and regulator guidance to prevent overreach. Pair policies with tiered learning and microlearning, localised for global teams and designed for neurodiverse employees, using scenarios grounded in your operations - sales dinners, field visits, night shifts, and customer escalations.

Internally, define roles and escalation paths for managers, HR, legal, and compliance so no one improvises under pressure. Managers are the first line of culture and control. Equip them with concise playbooks that cover in the moment intervention, impartial documentation, escalation routes, and support for targets and witnesses.

Managers should be trained to recognise subtle behaviours (exclusionary banter, tone policing, microaggressions, persistent late night criticism) and to set norms for digital communication across channels, hours, and tone.

Run proactive climate checks after reorganisations, performance cycles, or social events when risks spike. Use exit interviews, absence reviews, and pulse surveys to surface patterns early, and log all signals in a central system to detect trends before incidents escalate.

Close the loop with visible action:

- Targeted refreshers in hotspots
- Leadership presence
- Environmental changes where risks persist

Consistent, fair, timely action builds belief in the system and prevents trust attrition.

Governance and documentation form the backbone of reliable execution. State positions on dignity at work, anti harassment, whistleblowing, and third party conduct in concise, usable policies, and maintain a single source of truth with version control.

Assign mandatory reading with deadlines, collect attestations, and store records alongside training completions to create an auditable trail.
It is vital to make training continuous, short form, and context rich so it is recalled under pressure. Deliver three to five minute modules with a single objective, one or two questions, and a discussion prompt; sequence by role and risk and reference policies at the point of learning.

Building training as a priority

For teams without individual IT access (manufacturing, warehouses, hospitality) use huddles, canteen sessions, and rotating screens with captioned videos.

Provide printable posters and pocket guides for quick refreshers on standards and reporting. Track participation via roster uploads or QR check ins to maintain complete records. Measure understanding with brief knowledge checks and sentiment polls to catch misconceptions early, then reinforce with regular nudges, seasonal campaigns, and scenario discussions rooted in real operations to build muscle memory.

Sustain results through alignment and repetition. It is important to train staff on the value of speaking up. From there, make speaking up the pressure release valve for culture and risk. Provide multiple channels, anonymous and named, supported by a clear process: triage, visibility, timelines, confidentiality.

Train managers to route concerns correctly; one poor response can silence a team. Embed speak up guidance in policies and training, include examples that normalise raising concerns about peers, managers, and third parties, and ensure commercial terms enable intervention with external misconduct.

Share aggregate outcomes to show reporting leads to action. When these elements operate as a system, the number of incidents fall, issues resolve faster, and trust scales.

skillcast

About us

We help companies foster compliance awareness and encourage their employees to act with integrity. Our offering includes bespoke e-learning content development, a comprehensive library of ready-made courses, and a digital platform purpose-built for compliance training. More than 1,400 companies rely on our digital products each year to deliver millions of learning interventions.

Our SaaS portal streamlines GRC management by integrating learning content, activity tracking, policy management, and compliance submissions. By developing all technology and content in-house, we deliver tailored solutions that empower firms to simplify staff compliance, meet regulatory requirements efficiently, and minimise risk. Clients benefit from both custom e-learning and our extensive course libraries, using our platform to support their compliance training needs year after year.

"Everybody at Skillcast works towards a common goal: to give businesses exactly what they need to succeed in compliance management. With our technology and expertise, we help to build ethical and resilient workplaces and play a key role in creating a more compliant business landscape."

Vivek Dodd, CEO
Skillcast

Start your free trial

ERA Package