

Whistleblowing Policy

Policy · UK · Updated 2026-07-23 · Square brackets are placeholders to replace with your own details.

A whistleblowing policy is the written route for workers to report suspected wrongdoing inside your organisation — illegality, danger, fraud, cover-ups — safely and to the right person, so problems surface early instead of festering or leaking. It exists for concerns about the organisation and its impact on others, not for personal workplace disputes.

Most serious organisational failures were visible to someone on the inside long before they became public. The point of this policy is to make speaking up feel routine and safe: a named route, a promise of protection, and visible evidence that concerns are taken seriously.

This template covers what to report, how to raise a concern openly, confidentially, or anonymously, how your organisation investigates, the protection whistleblowers get, and when going to an outside regulator is appropriate.

Purpose and scope

This policy explains how anyone working for [Your company] — employees, workers, agency staff, contractors, and volunteers [adjust to your workforce] — can raise a concern about suspected wrongdoing within the business.

It does not replace other procedures: complaints about your own employment or treatment belong in the grievance procedure or the bullying and harassment policy, and customer complaints follow the complaint handling procedure. Where a concern contains both elements, we will separate them and handle each under the right policy.

Policy statement

[Your company] wants wrongdoing reported, however uncomfortable that is. We would always rather hear about a problem from our own people than from a regulator, a journalist, or a court. Anyone who raises a genuine concern under this policy will be supported and protected, even if the concern turns out to be mistaken.

What to report under this policy

- Criminal activity, including theft, fraud, or bribery.
- Failure to comply with a legal or regulatory obligation.
- Danger to the health and safety of any person — staff, customers, or the public.
- Damage to the environment.
- A miscarriage of justice.
- Misuse of personal data or serious breaches of confidentiality.
- Deliberate concealment of any of the above.

How to raise a concern

1. Report the concern to [whistleblowing officer — name/role]. If the concern involves that person, go to [alternative senior name/role] instead.
2. Raise it in writing or verbally — a conversation is a valid report and will be written up and confirmed back to you.
3. Give what facts you can: what you saw or heard, dates, people involved, and any documents. You are not expected to investigate or prove anything yourself.
4. Say whether you want to be identified, kept confidential, or remain anonymous. Anonymous reports are accepted, but they limit how well we can investigate and mean we cannot update or protect you directly.

How {{org.name}} handles concerns

1. Acknowledge the concern within [number] working days.
2. Make an initial assessment and decide the response: internal investigation, escalation to [owner/board], or referral to the police or a regulator.
3. Appoint an investigator with no involvement in the matter, who gathers evidence proportionately and confidentially.
4. Keep the person who raised the concern updated where possible — timescales and, as far as confidentiality allows, the outcome.
5. Record the concern, the investigation, and the outcome in [confidential register/location], and fix any process gap the case exposed.

Protection and confidentiality

Nobody who raises a genuine concern under this policy will be dismissed or suffer any detriment for doing so — no demotion, victimisation, lost hours, or exclusion. Retaliating against a whistleblower is a disciplinary offence at [Your company], and serious retaliation is gross misconduct.

We keep the identity of the person raising the concern confidential wherever we can. Deliberately false or malicious reports — as opposed to honest concerns that prove unfounded — are dealt with under the disciplinary procedure.

External disclosures

We hope anyone with a concern raises it internally first, so we can act quickly. However, workers have the legal right to make a protected disclosure to a prescribed person — the relevant regulator for the subject matter, such as the HSE for safety concerns or the ICO for data concerns. GOV.UK publishes the full list.

Nothing in this policy, any contract, or any settlement agreement prevents a worker from making a protected disclosure.

Records and review

The whistleblowing register is held by [name/role], access-restricted, and retained in line with our data retention policy. [Owner/board] reviews anonymised themes [frequency] so patterns are spotted.

This policy is reviewed [frequency, e.g. annually] and after every concern raised under it. Owner: [name/role]. Next review due: [date].

How to use this template

1. Name a whistleblowing officer and a genuinely independent alternative — the alternative route is the one that matters when the concern involves leadership.
2. Decide how anonymous reports can reach you in practice (a letter, a form, a voicemail box) and state it in the policy.
3. Brief managers that concerns may reach them first, and that their only job at that moment is to listen, record, and pass it to the named officer.
4. Publish the policy where staff actually look — induction, handbook, noticeboard — not only in a policy folder.
5. Test the route once a year: walk a hypothetical concern through the steps and check every named person still exists and knows their part.

Official guidance

- › [GOV.UK — Whistleblowing for employees](#)

This template is provided in good faith and for general information — it is not legal advice. Adapt it to your organisation and, where your sector carries specific legal requirements, have the finished document reviewed by a qualified adviser. The live version at <https://trainedteam.com/templates/whistleblowing-policy> is kept current; this file is a snapshot.