

Online Safety, Reporting and Appeals Policy

COLLABOR TECHNOLOGIES LTD

Company number 16888312 | Registered in England and Wales

Last Edited 1 September 2026

This policy explains how COLLABOR TECHNOLOGIES LTD (“Collabor”, “we”, “us” or “our”) receives safety reports, moderates content, takes account action, handles complaints and appeals, cooperates with law enforcement, and protects children. It applies to the Collabor platform, including profiles, campaign briefs, messages, uploaded files, deliverables, comments, reviews, contracts and other user-generated or user-shared content.

1. Who we are

COLLABOR TECHNOLOGIES LTD is a company registered in England and Wales under company number 16888312. Its registered office is Egerton Mill, 25–27 Egerton Street, Chester, United Kingdom, CH1 3ND.

Collabor connects brands and agencies with creators. Collabor provides tools for creator discovery, campaign management, messaging, uploads, contracting, payment protection and related support. Brands, agencies and creators remain responsible for their own campaign relationship and for complying with applicable law.

2. Scope of this policy

This policy applies to all people who access or use Collabor, anyone whose rights or safety may be affected by content on Collabor, and anyone who submits a report or complaint. It applies whether content is public, visible only to selected users, contained in one-to-one or group messages, or stored in campaign workspaces.

This policy should be read with Collabor’s Platform Terms, Brand Platform Agreement, Creator Platform Agreement, Acceptable Use and Content Standards, Privacy Notice and any campaign contract. If these documents conflict on a safety issue, Collabor may apply the provision that provides the stronger lawful protection while the conflict is reviewed.

A restriction under this policy is separate from a commercial dispute about campaign quality, deadlines or payment. The same facts may, however, raise both a safety issue and a commercial dispute.

3. UK online-safety position

For the purposes of this policy, Collabor treats at least its messaging and user-upload functions as a user-to-user service under Part 3 of the Online Safety Act 2023 because content generated, uploaded or shared by one user may be encountered by another user. The Act can apply to services of any size where they have links with the United Kingdom.

Collabor keeps the scope of its services and its applicable legal duties under review, including the service boundaries, UK links, relevant exclusions, creator-discovery functions and material product changes.

Collabor operates its UK-facing user-to-user functions on the basis that the relevant duties apply, unless a documented legal assessment establishes otherwise.

4. Our safety principles

- **Legality:** we act against content and conduct where we have reasonable grounds to infer that it is illegal, and against content that breaches our contractual rules even where it is not necessarily illegal.
- **Safety by design:** we assess how platform features may be misused and adopt proportionate safeguards, rather than relying only on reports after harm occurs.
- **Prompt action:** we prioritise imminent danger, child sexual exploitation or abuse, terrorism, credible threats, trafficking, intimate-image abuse, severe harassment and fraud.
- **Context and fairness:** we consider content, surrounding messages, metadata, user reports, the affected person's account, credible supporting material and reasonably available context.
- **Proportionality:** we match action to severity, likelihood, reach, recurrence, vulnerability and the need to prevent further harm.
- **Privacy and freedom of expression:** we avoid unnecessary intrusion or removal and give particular care to lawful journalistic, political, religious and artistic expression, while enforcing Collabor's ban on political campaigns and other platform rules.
- **Accountability:** we record material decisions, train relevant staff, review outcomes and correct errors.

5. Content and conduct we act against

Collabor may act against anything prohibited by law, the Acceptable Use and Content Standards, the platform agreements or this policy. This includes suspected content or conduct connected with:

- terrorism; child sexual exploitation or abuse; grooming; trafficking; sexual exploitation; extreme pornography; intimate-image abuse; cyberflashing; and coercive or controlling behaviour;
- credible threats, stalking, harassment, hate offences, incitement to violence, discriminatory abuse and serious self-harm offences;
- fraud, scams, impersonation, identity misuse, fake metrics, deceptive endorsements, money laundering, proceeds of crime and attempts to evade payment controls;
- illegal drugs, weapons, unlawful immigration services, sanctions evasion, foreign interference, hacking, malware and other cyber offences;
- adult or sexual content, political campaigns, weapons campaigns, spam, platform manipulation, review manipulation and unauthorised scraping or automation; and
- any campaign, product, claim or communication that breaches advertising, consumer-protection, intellectual-property, privacy, employment, tax, sanctions or other applicable law.

This list is illustrative, not exhaustive. Collabor may restrict lawful content that is nevertheless outside the platform's permitted purpose or creates unacceptable risk.

6. Child-safety position

6.1 Adults-only service

Collabor is designed for users aged 18 or over. A person under 18 must not register, access an account, negotiate a campaign, provide services through Collabor or communicate with users through the platform. An adult must not create or operate an account for a child.

An 18+ statement in terms is not, by itself, highly effective age assurance. Collabor completes a documented children's-access assessment for each relevant service or separable part. Where the

evidence requires it, Collabor introduces proportionate age assurance and access controls or complies with the additional children's duties that apply to a service likely to be accessed by children.

6.2 Zero tolerance for child sexual exploitation and abuse

Collabor prohibits child sexual abuse material, grooming, sexual communication with a child, sexual exploitation, trafficking, sextortion, solicitation of intimate images, instructions that facilitate abuse, and attempts to move a suspected child to another service for an improper purpose.

Users must not download, copy, retain, forward or re-upload suspected child sexual abuse material in order to make a report. A report should identify the account, message, campaign or link and explain the concern without reproducing illegal imagery.

6.3 Children appearing in campaign content

Although children cannot be Collabor users, a campaign deliverable may depict a child only where the responsible Brand or Agency and Creator have obtained every legally required consent, licence, permit and safeguarding approval; a parent or lawful guardian has given informed written consent; the activity and working conditions are lawful and age-appropriate; and the content is not sexualised, exploitative, dangerous, humiliating or otherwise harmful.

Collabor may require supporting evidence, impose additional restrictions or refuse or remove any campaign involving a child. A commercial agreement or parental consent does not override child-protection law or Collabor's safety judgement.

6.4 Suspected underage users

Collabor may request age-assurance evidence, restrict an account while checking eligibility, close an account reasonably believed to be operated by a child, preserve relevant records and make any report required by law. We seek to minimise the personal data collected for age assurance and explain the processing in the Privacy Notice.

7. How to report a safety concern

A user or other affected person may report content they reasonably believe is illegal or unsafe, a suspected child-safety issue, or a breach of Collabor's rules. Reports may be submitted through the in-platform Report function or Collabor's Help Centre contact route.

A report should include, where available:

- the relevant profile, username, campaign, message thread, file, deliverable or URL;
- what happened and why the reporter considers it illegal, unsafe or against Collabor's rules;
- when it occurred and whether it is continuing;
- whether anyone is in immediate danger or is believed to be under 18;
- any relevant jurisdiction or relationship between the people involved; and
- supporting screenshots or documents that can be shared lawfully and safely.

Reports may be made by the person directly affected, another user, a representative, a trusted organisation, law enforcement or another third party. Collabor may ask for more information but will not require unnecessary evidence before taking urgent protective action.

Collabor will not require a reporter to confront the reported user. Knowingly false or malicious reports may themselves breach Collabor's rules, but a good-faith report will not be penalised merely because it is not

upheld.

8. Emergencies and immediate danger

If someone is in immediate danger, call 999 in the United Kingdom or the appropriate emergency service where the person is located. In the UK, non-emergency crime may be reported to police on 101. Suspected child sexual abuse images or videos may also be reported to the Internet Watch Foundation.

After contacting emergency services, a reporter may alert Collabor so that we can preserve evidence and take platform action. Collabor cannot provide emergency, medical, safeguarding or legal services and cannot guarantee that a platform report will be reviewed in real time.

9. What happens after a report

9.1 Intake and triage

Collabor will record the report, protect it against unauthorised access, screen for urgency and conflicts of interest, and assign a priority. Where reasonably practicable, we will acknowledge receipt and provide a reference.

9.2 Review

A trained reviewer may examine the reported content and relevant information reasonably available to Collabor. This may include nearby messages, upload history, account information, campaign context, transaction records, previous reports, technical indicators and information supplied by affected people.

Collabor may use automated tools to detect, prioritise, limit or remove content, but material decisions should receive human review where appropriate to the risk, the reliability of the tool and the consequences for the user. Automated indicators are not treated as conclusive in every case.

9.3 Interim protection

While reviewing a concern, Collabor may temporarily hide content, restrict messaging, freeze a campaign workflow, pause a payment release where permitted by the Payments and Payout Protection Policy, block contact between users, preserve records or suspend an account. Interim action does not determine a campaign-payment dispute and does not imply criminal wrongdoing.

9.4 Decision standard

For duties requiring an illegal-content judgement, Collabor will apply the statutory 'reasonable grounds to infer' standard using relevant information reasonably available to it and Ofcom's current guidance. For contractual enforcement, Collabor may act where it reasonably concludes that content or conduct breaches its rules or creates an unacceptable platform risk.

9.5 Outcome

Where appropriate and lawful, Collabor will tell the reporter whether action was taken and tell an affected user the main reason for a restriction. We may withhold detail where disclosure could endanger someone, reveal confidential information, compromise detection systems, prejudice an investigation, breach law or enable further abuse.

10. Moderation and enforcement actions

Depending on the circumstances, Collabor may:

- take no action, monitor the issue or ask for more information;
- warn or educate a user and require corrective action;
- remove, disable, de-index, quarantine or restrict content or access to it;
- limit discovery, messaging, uploads, invitations, campaign activation, withdrawals or other features;
- pause or cancel a campaign workflow where permitted by the applicable agreements;
- temporarily suspend or permanently close an account;
- apply a device, payment, identity or re-registration restriction;
- preserve information and refer the matter to a payment provider, regulator, safeguarding body or law-enforcement agency; or
- take any other lawful and proportionate action reasonably necessary to protect users, Collabor or the public.

Collabor may act without advance notice where delay could increase harm, evidence could be lost, notice is legally prohibited, fraud or sanctions risk is suspected, or urgent action is otherwise reasonably necessary. Outstanding contractual and payment obligations may survive suspension or closure.

Repeat or coordinated violations, evasion, retaliation against a reporter, interference with an investigation and attempts to create replacement accounts are aggravating factors.

11. Complaints and appeals

11.1 Who may complain

Users and other affected people may complain about an alleged failure to act on suspected illegal content, the operation of the reporting process, a moderation outcome, the use of relevant automated technology, or another matter that Collabor is legally required to accept. A user may also appeal a decision affecting their own content, campaign access, features or account.

11.2 How to complain or appeal

Use the in-platform appeal or complaint route shown with the decision or Collabor's Help Centre contact route. An appeal by a user against a notified decision should normally be submitted within 14 calendar days. Collabor may accept a later appeal where fairness, disability, safety, delayed notice or another reasonable circumstance justifies it.

The request should identify the decision or report reference, explain the alleged error and provide any new information. Accessibility support or a reasonable adjustment may be requested.

11.3 Review process

Where practicable, a person who was not the original decision-maker will review a material appeal. The reviewer will consider the applicable rule, available evidence, context, proportionality, consistency, user safety, privacy and freedom of expression. Collabor may keep an interim restriction in place while the review is ongoing.

11.4 Possible outcomes

Collabor may uphold, vary or reverse the decision; restore or further restrict content or access; correct an account record; request additional action; or refer the matter for specialist or legal review. We will communicate the outcome and a concise reason where lawful and appropriate.

An appeal is not a substitute for a court, regulator, law-enforcement process or contractual dispute procedure. Collabor may decline repetitive, abusive, fraudulent or clearly out-of-scope submissions, but will preserve any complaint right required by law.

12. Law enforcement, regulators and safeguarding bodies

Collabor may preserve and disclose information where required by law, compelled by a valid legal process, necessary to protect vital interests, or otherwise permitted under applicable data-protection law. We will seek to verify the requester's identity and authority, assess jurisdiction and scope, disclose no more than reasonably necessary, and record material requests.

We may make proactive referrals where required or legally permitted, including reports concerning child sexual exploitation or abuse, credible threats to life, terrorism, trafficking, serious fraud or other serious offending. Where notification could increase risk or prejudice an investigation, Collabor may delay or omit notice to the affected user.

From 7 April 2026, in-scope user-to-user providers are required to report qualifying detected and previously unreported child sexual exploitation and abuse content to the UK National Crime Agency. Where this duty applies to Collabor, we will report qualifying content in accordance with the applicable regulations, including through the NCA's CSEA Industry Reporting Portal.

Law-enforcement and regulator requests should be submitted through Collabor's official-request route in the Help Centre. That route is for authorised official requests and emergencies, not ordinary customer support. In a UK emergency, authorities and members of the public should use 999.

13. Evidence, confidentiality and privacy

Collabor may retain reports, relevant content, messages, metadata, account records, moderation notes and decision history for as long as reasonably necessary for safety, legal compliance, dispute handling, fraud prevention and the establishment, exercise or defence of legal claims. Retention periods and lawful bases are described in Collabor's Privacy Notice and internal retention schedule.

Access will be limited to authorised personnel and service providers with a need to know. Collabor may share information with payment providers, identity or age-assurance providers, professional advisers, insurers, regulators, safeguarding bodies and authorities where lawful and necessary.

Reporters should not assume they are anonymous. Collabor will protect their identity where reasonably possible, but information may need to be disclosed to investigate fairly, comply with law or protect a person. We will avoid telling a reported user more than is necessary.

Safety monitoring and age assurance are subject to appropriate data-protection assessments, security measures, vendor due diligence and controls for international transfers.

14. Service integrity and abuse of safety systems

Users must not misuse reporting or appeals to harass, silence, threaten, obtain confidential information about, or gain a commercial advantage over another person. They must not destroy evidence, retaliate, coach false accounts, submit forged material or attempt to evade a restriction.

Collabor may combine related reports, prioritise new information, restrict abusive submissions and take action against misuse. We will not use this section to suppress good-faith reporting or a legally protected complaint.

15. Transparency, review and changes

Collabor will keep this policy and its associated risk assessments under review. Reviews should take place after a serious incident, a material change to features or user base, evidence of a new or increased risk, a significant regulatory change, or within any period required by law.

Where required, Collabor will ensure its terms explain the systems and processes used to protect users from illegal content and the policies governing reports and complaints. If Collabor becomes subject to additional categorised-service duties, it will update its disclosures and processes.

We may amend this policy to reflect legal, regulatory, operational or product changes. The current revision date appears at the top of this policy. Material changes will be communicated where required.

16. Contacting Collabor

Safety reports: use the Report function attached to the relevant content, message, profile or campaign, or the safety route in Collabor's Help Centre.

Complaints and appeals: use the link supplied with the decision or the complaints route in Collabor's Help Centre.

Legal and law-enforcement requests: use the official-request route in Collabor's Help Centre.

Post: COLLABOR TECHNOLOGIES LTD, Egerton Mill, 25–27 Egerton Street, Chester, United Kingdom, CH1 3ND.

Do not send suspected child sexual abuse images or videos to Collabor by email or post. Identify the relevant account, content or link without copying the material.