CLAAS2SAAS GROUP

Whistleblowing Policy

The CLaaS2SaaS Group is committed to the highest standards of ethical conduct. If you suspect wrongdoing, tell us. You can report safely, confidentially and, if you wish, anonymously.

SPEAK UP – FILL OUT FORM

EMAIL WB@CLAAS2SAAS.COM

Our commitment

We expect everyone who works with us to act honestly and fairly and to comply with the law, their contractual obligations and our policies. We take a zero-tolerance approach to fraud, corruption and unlawful behaviour.

This policy gives you a safe and confidential way to raise a concern about suspected wrongdoing. It applies to every company in the CLaaS2SaaS Group and is overseen by the Group Audit Committee.

Who can raise a concern

Anyone can raise a concern, including our staff, directors and part-time staff; student recruitment agents and academic partners; learners, vendors and suppliers; and members of the public.

What you can report

- Accounting, internal control or auditing irregularities
- Fraud, theft or misuse of assets
- Corruption, bribery or other unethical conduct
- Breaches of law or regulation

- Suspected or actual personal data breaches
- Workplace safety violations
- Abuse of authority
- Undisclosed conflicts of interest
- False reporting to regulators or stakeholders
- Misleading auditors or manipulating financial records
- Concealment of wrongdoing
- Any other misconduct that could cause financial or reputational damage

---

How to raise a concern

Use whichever channel you are most comfortable with.

ANYONE · ANONYMOUS WELCOME

Speak Up form

Report online, with or without your name.

Speak Up – Fill out form

ANYONE · ANONYMOUS WELCOME

Whistleblowing email

WB@claas2saas.com

Only the Chair of the Audit Committee can access this mailbox. Use it, or the Speak Up form, if you wish to stay anonymous or your concern involves the Head of Compliance. If your concern involves the CEO or senior management, you may report directly to the Audit Committee Chair here.

EMPLOYEES

Your line manager or Head of Business Unit

Raise it with them if you are comfortable doing so. They refer your concern to the Head of Compliance on the same working day.

EMPLOYEES AND DIRECTORS

Head of Compliance

Raise it directly with the Head of Compliance, without going through your line manager.

Concerns about HR matters may also be raised with the Head of HR, who refers any reportable matter to the Head of Compliance.

What to include in your report

- Your name and contact details (optional)
- The date, time and location of what happened
- The people involved
- A description of what happened
- Any supporting evidence

Anonymous reports are accepted and assessed, but we may be limited in how far we can investigate, and we can only tell you the outcome if you give us a way to contact you.

What happens after you report

1

We log your report WITHIN 1 WORKING DAY

The Head of Compliance records every report, whatever the channel, and assesses its seriousness and who should look into it.

2

We assess and acknowledge it WITHIN 3 WORKING DAYS

We assess whether the report is valid. If it is, we escalate it to the Chief Operating Officer and email you an acknowledgement, with our commitment that you will not suffer retaliation.

3

We escalate serious matters

Concerns about fraud, financial misconduct, safety or senior management go directly to the Audit Committee, and concerns about the CEO or senior

management are never routed through management. Personal data breaches are referred to our Data Protection Officer at once.

4

We investigate

Where needed, an Investigation Panel of people independent of the business unit and of anyone implicated investigates objectively and confidentially, following the principles of natural justice and fairness. The Audit Committee may also appoint external legal counsel, forensic specialists or other independent parties. No one implicated in, or with a conflict of interest in, the matter takes part in assessing or investigating it.

5

We decide and act

The panel finds the allegations substantiated, partially substantiated or unsubstantiated, and recommends any corrective, preventive, disciplinary or remedial action. The Chief Operating Officer, or the Audit Committee for escalated matters, decides the action.

6

We tell you the outcome WITHIN 30 WORKING DAYS

If you gave your contact details, we tell you the outcome by email, as far as confidentiality allows, within 30 working days of receiving your report. If the investigation takes longer, we keep you updated where practicable.

Confidentiality

Your identity is known only to the smallest number of people needed to investigate. If you report anonymously, we will not try to identify you. Personal data in a report is handled in line with our **Privacy Policy** and the Personal Data Protection Act 2012.

Protection from retaliation

Retaliation against anyone who reports a concern in good faith, including dismissal, demotion, harassment, discrimination, threats or any other adverse action, is a material breach of our Code of Conduct and leads to disciplinary action, up to termination. If you

are an employee, we monitor your employment status and treatment for 12 months after you report to detect any retaliation.

Reporting in good faith

Protection applies to reports made in good faith: honestly, with a reasonable belief that the information is true, and not for personal gain or with malicious intent. It does not apply to malicious or bad-faith reports, and anyone found to have made a malicious or knowingly false report may face disciplinary action.

Oversight

The Audit Committee oversees our whistleblowing arrangements. It receives regular reports on the number, themes and outcomes of concerns raised, and reviews this policy and our arrangements in line with Provision 10.4 of the Code of Corporate Governance 2018. We review the policy at least every two years, or earlier when regulations or our organisation change.

Last updated: 26 November 2026