



People & culture

Whistleblowing policy

How to raise a concern about wrongdoing, and how TLG will protect and support you

Version	2.0
Published	October 2026
Owner	Chief People Officer
Classification	Internal

Document control

Document title		Whistleblowing policy
Document reference		HR-00-02P
Version		2.0
Status		Draft for approval
Classification		Internal
Policy owner		Sally Bannister, Chief People Officer
Data protection contact		Tanya Taylor, Data Protection Officer
Approved by		Mark Sullivan, Chief Technology Officer
Approval date		October 2026
Effective date		October 2026
Next review		October 2027, or sooner if the law, ICO guidance or our processing changes

Version history

Version	Date	Author	Summary of changes
1.1	March 2023	Rachael Walsh-Grant	Previous Whistleblowing Policy.
2.0	October 2026	Tanya Taylor	Full rewrite: new TLG branding; review date overdue (January 2025); file path removed from header; scope extended; examples expanded (safeguarding, data protection, sexual harassment); grievance distinction; reporting routes table; meeting, investigation and feedback timescales; escalation route; prescribed persons; protection from detriment and NDAs; responsibilities; data protection and record-keeping section; monitoring

			and review; contacts and related documents; document control added.
--	--	--	---

Contents

1. Introduction and purpose	4
2. Scope	4
3. What is whistleblowing?	4
4. Raising a concern	5
5. Meetings and support	6
6. Confidentiality and anonymity	6
7. Investigation and outcome	6
8. If you are not satisfied	7
9. External disclosures	7
10. Protection and support	8
11. Responsibilities	9
12. Data protection and record-keeping	9
13. Training, monitoring and review	10
 Appendix A – Contact information	 11

1. Introduction and purpose

1.1 TLG (Transforming Learning Group) and its group companies (together "TLG", "we" or "us") are committed to conducting business with honesty and integrity, and we expect everyone who works with us to maintain high standards. We want a culture where people feel safe to speak up, and where concerns are listened to and acted on.

1.2 This Policy explains how to raise a concern about suspected wrongdoing or danger, how we will deal with it, and the protection available to you. Any suspected wrongdoing should be reported as soon as possible.

1.3 This Policy reflects the Public Interest Disclosure Act 1998, which inserted whistleblowing protection into the Employment Rights Act 1996, together with related legislation and guidance.

In brief

- **If you suspect wrongdoing or danger at work, speak up early. You do not need proof, only a reasonable belief.**
- **Raise it with your manager, the People & Culture team or your Managing Director, or with the Group Leadership Team if it involves senior managers.**
- **We will treat your concern confidentially, take it seriously and tell you what we can about the outcome.**
- **You will not suffer any detriment for raising a genuine concern, even if you turn out to be mistaken.**

2. Scope

2.1 This Policy applies to all employees, officers, directors, consultants, contractors, volunteers, interns, apprentices, casual workers and agency workers of TLG, whether current or former (together "staff").

2.2 We also encourage suppliers, customers and other third parties connected with our business to raise concerns under this Policy.

2.3 This Policy does not form part of any employee's contract of employment, and we may amend it at any time.

2.4 This Policy is not for personal grievances about your own employment, such as pay, workload or a dispute with a colleague. These should be raised under the Grievance Policy. If you are unsure which policy applies, speak to the People & Culture team.

3. What is whistleblowing?

3.1 Whistleblowing is the reporting of suspected wrongdoing or dangers in relation to our activities, or the activities of others connected with our business. This includes, for example:

- a) criminal activity, including fraud, theft, bribery and corruption, and the facilitation of tax evasion;
- b) failure to comply with any legal or regulatory obligation, including data protection law;
- c) miscarriages of justice;
- d) danger to the health and safety of any individual;
- e) risks to the safety or welfare of children or vulnerable adults;
- f) damage to the environment;
- g) modern slavery, human trafficking, forced labour or exploitation in our business or supply chains;
- h) sexual harassment, discrimination or other serious misconduct;
- i) serious breaches of our policies or professional standards, or conduct likely to damage TLG's reputation or the trust of our school and trust customers;
- j) misuse of, or serious risks to, personal data or information security; and
- k) the deliberate concealment of any of the above.

3.2 To qualify for legal protection, you must reasonably believe that the information you disclose tends to show one of these types of wrongdoing, and that the disclosure is in the public interest. This means it affects others, such as customers, pupils, colleagues, the public or the organisation itself, rather than being only a personal matter about your own employment terms.

3.3 You do not need firm evidence before raising a concern. A reasonable suspicion is enough. You should not carry out your own investigation.

3.4 Safeguarding. If your concern is about the immediate safety or welfare of a child or vulnerable adult, including in a school where you are working, you must also follow our Safeguarding Policy and the school's safeguarding procedures, and report it to the

school's Designated Safeguarding Lead without delay. If someone is at immediate risk, call 999.

4. Raising a concern

4.1 We hope that in many cases you will be able to raise a concern with your line manager, in person or in writing. However, if you prefer not to raise it with your manager for any reason, or you have done so and the concern has not been addressed, you can use any of the following routes:

Route	When to use it	Contact
Your line manager	First point of contact for most concerns	In person, by phone or by email
People & Culture team	Any concern, if you prefer not to speak to your manager, or need advice	Rachael Walsh-Grant – rachael.walsh-grant@transforming-learning.co.uk
Managing Director / business leader	Serious concerns within a TLG business	Sally Bannister – CPO – sally.bannister@transforming-learning.co.uk
Group Leadership Team / Chair or non-executive director	If the concern involves senior managers, a director or the Executive Leadership Team	Tom Welch – CEO, or Ben Marnham – Chairman
Data Protection Officer	Concerns about the misuse or security of personal data	Tanya Taylor – tanya.taylor@tlg.co.uk

4.2 When raising a concern, it helps if you can give as much of the following as possible: what happened, when and where, who was involved, any evidence or documents you are aware of, and whether anyone else knows about it. You do not need all of this to raise a concern.

4.3 Whoever receives the concern must pass it to the People & Culture Manager without delay, keep it confidential and must not try to investigate it themselves.

5. Meetings and support

5.1 The People & Culture team will arrange a meeting with you as soon as possible, normally within 5 working days of receiving your concern, to discuss it. The meeting can be held in person or remotely.

5.2 You may bring a colleague or trade union representative to any meeting under this Policy. Your companion must respect the confidentiality of your disclosure and any investigation.

5.3 We will take a written summary of your concern and give you a copy after the meeting. We will also explain how we propose to handle the matter and give you an indication of how long it is likely to take.

5.4 We know that raising a concern can be stressful. Support is available through Wellbeing Solutions on Bravo, your line manager or the People & Culture team.

6. Confidentiality and anonymity

6.1 We hope you will feel able to raise concerns openly. If you want to raise a concern confidentially, we will make every effort to keep your identity secret and will only share it with those who need to know in order to investigate or act on your concern. If it becomes necessary to reveal your identity, for example because we are required to by law, we will discuss this with you first wherever possible.

6.2 You can raise a concern anonymously, for example by letter. However, anonymous concerns can be harder to investigate, it may be more difficult to protect you, and we will not be able to give you feedback unless you give us a way to contact you. We encourage you to tell us who you are on a confidential basis instead.

6.3 Anyone involved in handling a concern must keep the information, and the identity of the whistleblower and anyone else involved, strictly confidential. Breaching confidentiality, or trying to identify an anonymous whistleblower, may result in disciplinary action.

7. Investigation and outcome

7.1 Once you have raised a concern, we will carry out an initial assessment to decide the scope of any investigation. The investigation will be carried out by someone independent of the matter, which may be an external investigator where appropriate.

7.2 We may need you to provide further information. We will aim to keep you informed of progress and of the likely timescale. Our target timescales are:

Stage	Target timescale
Acknowledge receipt of your concern	Within 3 working days
Initial meeting with you	Within 5 working days
Initial assessment and decision on next steps	Within 10 working days
Investigation completed and feedback given	Normally within 30 working days, depending on complexity. We will tell you if it will take longer.

7.3 Sometimes the need for confidentiality, including towards other people involved, may prevent us from giving you specific details of the investigation or any action taken. You should treat any information about the investigation as confidential.

7.4 If we find that wrongdoing has occurred, we will take appropriate action, which may include disciplinary action, reporting to the police or a regulator, notifying our customers where required, and changing our processes to prevent it happening again.

7.5 If the concern involves a personal data breach, it will also be handled under the Data Breach Policy, which has strict deadlines for reporting to the ICO. If it involves a safeguarding matter, our safeguarding procedures will take priority.

8. If you are not satisfied

8.1 While we cannot always guarantee the outcome you are seeking, we will try to deal with your concern fairly and appropriately.

8.2 If you are not happy with the way your concern has been handled, you can raise it with the People & Culture Manager or, if they were involved, with the Chief Executive Officer / Chair / a non-executive director, who will review how it was handled.

9. External disclosures

9.1 The aim of this Policy is to provide an internal way of reporting, investigating and putting right any wrongdoing. In most cases you should not find it necessary to alert anyone externally.

9.2 The law recognises that in some circumstances it may be appropriate for you to report your concerns to an external body, such as a regulator. Legal protection is usually available if you report to a prescribed person (a regulator or body listed by the Government) and you reasonably believe the information and any allegation in it are substantially true. Examples relevant to TLG include:

Prescribed person	Matters
Information Commissioner's Office	Data protection and freedom of information
HM Revenue & Customs	Tax and National Insurance
Health and Safety Executive	Health and safety at work
Serious Fraud Office	Serious or complex fraud and bribery
Ofsted	Children's services and education, including safeguarding
Competition and Markets Authority	Competition and consumer law
Your Member of Parliament	Any matter

9.3 A full list of prescribed persons is published on GOV.UK. Disclosures to anyone else, such as the media, are only protected in very limited circumstances, and you should not contact the media about a concern without taking advice first.

9.4 We strongly encourage you to seek advice before reporting a concern to anyone outside TLG. Protect, the independent whistleblowing charity, offers a free, confidential advice line (see **Appendix A**). You can also take advice from a lawyer or trade union.

9.5 Whistleblowing concerns usually relate to the conduct of our staff, but they may sometimes relate to the actions of a third party, such as a customer or supplier. We encourage you to report such concerns internally first.

10. Protection and support

10.1 We aim to encourage openness and will support staff who raise genuine concerns under this Policy, even if they turn out to be mistaken.

10.2 Whistleblowers must not suffer any detrimental treatment as a result of raising a concern. Detrimental treatment includes dismissal, disciplinary action, threats, bullying, being overlooked for promotion or work, or other unfavourable treatment. It is unlawful under the Employment Rights Act 1996 (as amended by the Public Interest Disclosure Act 1998) for a worker to be dismissed or subjected to any detriment because they have made a protected disclosure.

10.3 If you believe you have suffered any such treatment, you should tell the People & Culture Manager immediately, or your Managing Director if the People & Culture Manager is involved. If the matter is not put right, you should raise it formally using the Grievance Policy.

10.4 Staff must not threaten or retaliate against whistleblowers in any way. Anyone involved in such conduct will be subject to disciplinary action. In some cases, the whistleblower could bring a claim against the individual responsible as well as against TLG.

10.5 No agreement, including a settlement or non-disclosure agreement, can prevent you from making a protected disclosure, and nothing in your contract or any TLG policy is intended to do so.

10.6 If we conclude that a whistleblower has made an allegation they know to be false, or has acted maliciously, they may be subject to disciplinary action.

11. Responsibilities

Role	Responsibilities
Board / Executive Leadership Team	Overall responsibility for this Policy and for making sure concerns are dealt with properly; receive regular, anonymised reports on whistleblowing.
People & Culture Manager	Day-to-day responsibility for this Policy; receives and logs concerns; arranges

	investigations; makes sure whistleblowers are protected and receive feedback.
People & Culture team	Supports the People & Culture Manager, advises managers and staff, and handles related HR matters.
Managers	Listen to and pass on concerns promptly and confidentially; make sure no one in their team is subjected to detriment.
Data Protection Officer	Advises on handling personal data in whistleblowing cases and on any concerns involving personal data.
All staff	Raise concerns about wrongdoing; cooperate with investigations; keep information confidential; never victimise anyone who has raised a concern.

12. Data protection and record-keeping

12.1 Whistleblowing concerns and investigations involve personal data about the whistleblower, the people concerned and any witnesses. TLG will process this information in line with the UK GDPR, the Data Protection Act 2018, the Data (Use and Access) Act 2025 and our Data Protection Policy.

12.2 We process this information on the basis of our legal obligations and our legitimate interests in investigating and preventing wrongdoing. Where special category or criminal offence data is involved, we rely on the relevant conditions in Schedule 1 of the DPA 2018, including preventing or detecting unlawful acts.

12.3 Records of concerns, investigations and outcomes will be kept securely, with access limited to those who need it. They are kept for 6 years from the close of the investigation, in line with the Data Retention Policy, and then securely destroyed.

12.4 If someone makes a subject access request that includes information about a whistleblowing case, we will consider carefully whether information identifying the whistleblower or others should be withheld or redacted, in line with the exemptions in the DPA 2018 and our Data Subject Access Request Policy and Procedure. We will always seek to protect the identity of a whistleblower who has asked for confidentiality.

12.5 Questions about data protection in relation to whistleblowing should be directed to the DPO, Tanya Taylor, at tanya.taylor@tlg.co.uk.

13. Training, monitoring and review

13.1 All staff will be made aware of this Policy at induction. Managers and anyone with a role in handling concerns will receive appropriate training.

13.2 The People & Culture Manager will keep a confidential log of all concerns raised and will report anonymised information on the number and type of concerns, and their outcomes, to the Executive Leadership Team at least annually.

13.3 This Policy will be reviewed at least annually, and sooner if there are changes in the law or guidance.

13.4 This Policy is effective from October 2026 and has been approved and authorised by:

Name	Mark Sullivan
Position	Chief Technology Officer
Date	October 2026
Due for review by	October 2027

Appendix A – Contact information

Internal contacts

Contact	Details
People & Culture Manager	Rachael Walsh-Grant – rachael.walsh-grant@transforming-learning.co.uk
[Chair / non-executive director]	[contact]
Data Protection Officer	Tanya Taylor – tanya.taylor@tlg.co.uk

External advice and reporting

Organisation	Details
Protect (independent whistleblowing charity)	Advice line: 020 3117 2520 – Website: protect-advice.org.uk
Prescribed persons list	GOV.UK – “Whistleblowing: list of prescribed people and bodies”
Information Commissioner’s Office	0303 123 1113 – ico.org.uk
Action Fraud (to report fraud and cybercrime)	0300 123 2040 – actionfraud.police.uk
Modern Slavery & Exploitation Helpline	08000 121 700

Legislation

- Employment Rights Act 1996, Part IVA (as inserted by the Public Interest Disclosure Act 1998)
- Enterprise and Regulatory Reform Act 2013 (public interest test)
- Bribery Act 2010 and Criminal Finances Act 2017
- Modern Slavery Act 2015
- UK GDPR, Data Protection Act 2018 and Data (Use and Access) Act 2025

Related TLG documents

- Modern Slavery and Human Trafficking Policy
- Safeguarding Policy
- Anti-Bribery and Corruption Policy
- Data Protection Policy
- Grievance Policy
- Data Breach Policy
- Disciplinary Policy
- Information Security Policy