Message from Programmed

Speaking up about serious misconduct, unlawful conduct or other serious wrongdoing helps protect our people, customers, communities and business. Programmed treats SpeakUp reports seriously, fairly and confidentially. You do not need to prove wrongdoing. If you have reasonable grounds to suspect a serious concern, we encourage you to SpeakUp.

Purpose

Programmed is committed to high ethical standards, openness, accountability and fair treatment. This policy explains how you can raise serious concerns, how reports will be handled, and the protections that may apply under Australian and New Zealand law.

SpeakUp is the name of Programmed's dedicated confidential reporting channels and process. The word whistleblower is used only where needed to explain legislation or legal protections.

SpeakUp at a glance

Question	Plain English answer	What this means
What is SpeakUp?	A confidential way to report serious concerns.	It is not a replacement for ordinary people, payroll, safety, privacy or customer complaint processes unless serious wrongdoing or legal protection may be involved.
Who can SpeakUp?	Current and former employees, officers, contractors, contractor employees, suppliers, associates and some connected people.	Australian law also covers certain relatives and dependants. New Zealand law covers people with a work-related connection.
What can I report?	Suspected misconduct, fraud, corruption, unlawful conduct, serious safety or environmental risks, victimisation, or an improper state of affairs.	You need reasonable grounds for the concern, but you do not need proof.
Can I be anonymous?	Yes.	Programmed will respect anonymity. It may be harder to investigate or provide feedback if there is no safe way to contact you.
How do I report?	Email, phone, mail or someone who can receive SpeakUp reports, such as certain senior Programmed leaders, regulators or lawyers.	Email speakup@programmed.com.au; call 1300 035 808 in Australia or 0800 950 450 in New Zealand.
Will I be protected?	Programmed prohibits retaliation and protects confidentiality.	Legal protections vary by jurisdiction and circumstances, and may include immunity and access to remedies.

When to use SpeakUp

Use SpeakUp when you have reasonable grounds to suspect serious wrongdoing in relation to Programmed, including:

- fraud, theft, bribery, corruption, dishonest conduct, money laundering or a serious conflict of interest
- a serious breach of law, regulation, licence condition or Programmed policy
- a serious risk to health, safety, public safety, the environment, consumers, customers or the community
- misconduct, negligence, breach of trust, breach of duty or an improper state of affairs
- victimisation, retaliation, threatened detriment or a breach of confidentiality connected with a SpeakUp report
- conduct that may significantly affect Programmed, its people, customers, regulators or reputation
- serious cyber security misconduct, deliberate concealment of a material incident, or misuse of systems or information

If you are unsure

Do not investigate the matter yourself. Contact the APAC Regional Director - Risk & Compliance, RM Risk and Compliance or someone who can receive SpeakUp reports, such as certain senior Programmed leaders, regulators or lawyers. Programmed will assess the right process and any protections that apply.

Matters usually handled through other channels

The following matters are usually handled through other Programmed processes unless they also involve serious wrongdoing, illegality, victimisation, a breach of whistleblower protections or wider implications for Programmed:

- personal work-related grievances, including ordinary interpersonal conflict, performance management, rostering, pay queries or individual employment decisions
- privacy queries or data breach matters
- work health and safety incidents, hazards and injuries
- customer complaints or operational service issues
- people-related complaints suitable for a manager, People and Culture, Open Door or another workplace process
- If a report is made through SpeakUp but another process is more appropriate, Programmed will first consider whether legal protections apply, then refer or manage the matter while protecting confidentiality as required.

How to make a SpeakUp report

Reports may be verbal, written or electronic. Share as much information as you safely can, such as what happened, when, who was involved, possible witnesses, available records and whether anyone is at immediate risk.

Speak Up channel	Details
Email	speakup@programmed.com.au
Phone	Australia: 1300 035 808 New Zealand: 0800 950 450
Mail	Private and Confidential Attn: 226 Adelaide Terrace, Perth CBD 6000
Other people who can receive SpeakUp reports	This may include a Programmed director, officer or senior manager; the Company Secretary; an auditor or audit team member; an actuary; ASIC, APRA or another prescribed Commonwealth authority; an appropriate New Zealand authority; or a legal practitioner for advice about whistleblower protections

Anonymous reports

You may report anonymously and remain anonymous during and after the process. Programmed will take reasonable steps to protect information that may identify you. If possible, use a method that allows safe two-way contact so questions, support and updates can be provided.

What happens after you report

1. **Receive and assess:** Where contact details are available, the report will be acknowledged. The authorised recipient will assess the concern, applicable law, immediate risks and the appropriate process.
2. **Plan protections:** Programmed will consider confidentiality, risk of detriment, safety, wellbeing support, conflicts of interest and any interim safeguards.
3. **Plan the response:** If investigation is appropriate, a suitably independent investigator will be appointed and the scope, evidence, communication and confidentiality controls will be defined.
4. **Investigate fairly:** Relevant evidence will be considered. People affected by adverse information will be given a fair opportunity to respond before final findings, where lawful and safe.
5. **Act and close:** Programmed will decide what action is required, address substantiated wrongdoing, and provide updates or outcome information where appropriate and legally permitted.
6. **Learn and report:** De-identified themes and outcomes may be reported to management or the Board to address systemic risks and improve controls.

Support and protection from detriment

Programmed will not tolerate anyone causing or threatening detriment because a person has made, may make, proposes to make, or is suspected of making a SpeakUp report. Detriment may include dismissal, demotion, disciplinary action, harassment, intimidation, discrimination, disadvantage, reputational harm, financial harm or other adverse treatment.

Support may include confidentiality planning, wellbeing support, changes to reporting lines or work arrangements, conflict management, reminders about expected conduct, and disciplinary action for retaliation or confidentiality breaches.

Confidentiality

Programmed will protect a reporter's identity and information likely to identify them, except where disclosure is permitted or required by law. Information will be limited to people who need it for assessment, investigation, legal advice, regulatory reporting, risk control or support. Where identifying information is reasonably necessary for an investigation, Programmed will take reasonable steps to reduce the risk of identification.

Fair treatment of people named in a report

A report is an allegation unless and until facts are established. Programmed will act discreetly and objectively, with appropriate regard to confidentiality, privacy, procedural fairness and wellbeing. A person facing a possible adverse finding will be given a reasonable opportunity to respond before a final decision, unless this would be unlawful, unsafe or likely to compromise the investigation.

Reports that are not substantiated or are knowingly false

A person will not be disadvantaged for making a report where they have reasonable grounds to suspect wrongdoing, even if the concern is not substantiated. Knowingly false or malicious reports may result in disciplinary action. Making a report does not protect a person from the consequences of their own misconduct revealed by the report.

Legal protections

This policy is intended to align with applicable whistleblower and protected disclosure laws. If this policy is inconsistent with the law, the law prevails. People considering an external, public interest or emergency disclosure should obtain independent legal advice.

Australia: Corporations Act 2001

- An eligible whistleblower may include a current or former officer, employee, contractor, contractor employee, supplier or associate, and certain relatives or dependants.
- A qualifying disclosure may concern misconduct, an improper state of affairs or circumstances, certain financial sector or Commonwealth offences, danger to the public or financial system, or victimisation connected with a protected disclosure.
- A disclosure may be made anonymously and protections can apply whether or not the concern is substantiated, provided there were reasonable grounds for suspicion.
- Reports may be made to someone who can receive SpeakUp reports, such as officers, senior managers, auditors, actuaries, ASIC, APRA, prescribed Commonwealth authorities and legal practitioners for advice about whistleblower protections.
- Protections may include confidentiality, protection from detriment, compensation and other remedies, and protection from certain civil, criminal, administrative or disciplinary liability for making the disclosure.
- Personal work-related grievances are generally excluded unless they have wider implications, involve victimisation, or otherwise meet the statutory criteria.
- Public interest and emergency disclosures to a journalist or parliamentarian are protected only in limited circumstances and have specific preconditions.

New Zealand: Protected Disclosures (Protection of Whistleblowers) Act 2022

- The Act applies to all organisations and protects people who disclose serious wrongdoing in or by their organisation in accordance with the Act and not in bad faith.
- Serious wrongdoing includes offences; serious risks to public health, public safety, individual health and safety or the environment; serious risks to the maintenance of law; unlawful, corrupt or irregular use of public funds or resources; and certain serious public sector misconduct.
- A protected disclosure may be made using internal procedures or to an appropriate authority.
- Protections include confidentiality, protection from retaliation and victimisation, immunity from civil, criminal and disciplinary proceedings for making the disclosure, and no contracting out.
- A receiver should acknowledge, consider and deal with a protected disclosure within 20 working days where practicable, and provide updates if additional time is needed.

Records, governance and reporting

SpeakUp reports will be recorded and managed securely using Programmed's approved workflow or case management process. Access is limited to authorised people with a legitimate role in assessment, investigation, legal advice, oversight, risk management or support.

De-identified insights may be reported to senior management and the Board to monitor trends, identify systemic risks, check that protections are working and support continuous improvement. A reporter will not be identified unless disclosure is legally permitted and appropriate controls are in place.

Availability, training and review

This policy will be available through appropriate channels, including the intranet, websites, induction and training materials. Awareness activities will be suitable for desk-based and non-desk-based workers.

The policy will be reviewed at least every three years, after relevant legislative change, after a material change to SpeakUp channels or investigation processes, or following significant lessons from a review or case. Amendments require approval under Programmed's document governance requirements.

Review

At least every 3 years, following legislative change, or after a material change to SpeakUp

Appendix A: Common Questions

Question	What to do
Do you suspect serious misconduct, unlawful conduct, corruption, fraud, serious safety or environmental risk, victimisation or an improper state of affairs?	Use SpeakUp or contact someone who can receive SpeakUp reports, such as certain senior Programmed leaders, regulators or lawyers
Is the concern mainly a personal work-related grievance with no wider serious wrongdoing or victimisation issue?	Use your manager, People and Culture, Open Door or the relevant workplace process.
Are you unsure which channel applies?	Contact the APAC Regional Director - Risk & Compliance or someone who can receive SpeakUp reports, such as certain senior Programmed leaders, regulators or lawyers. Programmed will triage the matter.
Is someone at immediate risk?	Take urgent action first, including emergency services or local safety escalation, then report through the appropriate channel.

Appendix B: Legislative and Regulatory References

- Corporations Act 2001 (Cth)
- ASIC Regulatory Guide 270: Whistleblower policies
- ASIC: Protections for corporate sector whistleblowers
- Protected Disclosures (Protection of Whistleblowers) Act 2022 (NZ)
- NZ Ombudsman: Guidance for receivers