Crimson Global Academy

Online Safety Policy

Purpose

Crimson Global Academy ("CGA") is committed to providing a physically and emotionally safe place for all students and staff in every environment where teaching and learning happen — including our virtual classrooms and digital platforms. Our goal is to create an inclusive online school culture where students feel connected, respected, and supported to achieve their best while being protected from harm.

This policy sits alongside the Safeguarding and Child Protection Policy, Student Code of Conduct Anti-Bullying Policy, Privacy Policy, Safe and Inclusive Learning Environment Policy, and the Enrolment Terms. Together, these ensure Crimson Global Academy meets its obligations under the Education and Training Act 2020 & other applicable regulations, rules, expectations, and guidance.

Scope

This policy applies to all members of Crimson Global Academy's community whenever they are participating in CGA learning or activities, whether during scheduled class time or other school-related interactions. It covers:

- School-provided digital platforms, accounts, tools, and devices.
- Privately owned devices and internet connections used for school learning.
- All virtual classrooms, learning management systems (LMS), video-conferencing environments, messaging, forums, email, collaborative documents, and any other digital spaces the Academy uses.
- Online conduct that affects student/staff safety or the school environment, even if it occurs off-platform or outside school hours.

Guiding Principles

Crimson Global Academy's online safety approach is grounded in:

1. **Prevention first**: building safe norms, literacy, and relationships is more effective than relying on discipline after harm.
2. **Shared responsibility**: students, staff, whānau/caregivers, and the school all have roles in keeping digital spaces safe.

3. **Learn – Guide – Protect**: reflecting Netsafe's framework for online safety education and risk reduction.
4. **Manaakitanga and inclusion**: online spaces must be free from racism, discrimination, harassment, and bullying, and support learner wellbeing.
5. **Privacy and dignity**: safety measures must respect privacy and follow lawful, proportionate monitoring practices.
6. **Accessibility and equity**: online safety must work for diverse learners and home contexts, including limited bandwidth, shared devices, disability, neurodiversity, and cultural needs.

Legal and Regulatory Context

CGA operates in full compliance with its obligations, and follows guidance from relevant agencies, including:

- **Education and Training Act 2020**: the school has an overarching responsibility to create and maintain a safe physical and emotional environment for its students and staff.
- **Health and Safety at Work Act 2015**: the school's governing board must take reasonably practicable steps to manage risks, including those arising in an online context.
- **Privacy Act 2020**: the school must only collect, use, disclose, store, and access personal information in accordance with the law.
- **Harmful Digital Communications Act 2015**: the school should make students aware of appropriate online behaviour and the digital communication principles.
- Ministry of Education and Netsafe digital safety/cybersecurity guidance.

Role and Responsibilities

Board / Governing Body

- Approves this policy and reviews it annually.
- Ensures adequate resourcing for online safety and cybersecurity.

Principal

- Ensures implementation and staff capability.
- Oversees significant incidents and reporting to the Board.
- Liaises with whānau and external agencies where appropriate.
- Provides guidance and staff support.

Designated Safeguarding Lead (DSL)

- Coordinates prevention, response, and incident recording.
- Liaises with whānau and external agencies where appropriate.
- Provides guidance and staff support.
- Takes other appropriate steps in line with our Safeguarding and Child Protection Policy

All staff

- Model safe and respectful digital behaviour.
- Use only CGA-approved platforms to communicate with students.
- Act on and report safety concerns promptly.

Students

- Follow the Student Code of Conduct.
- Comply with the Technology Use and Online Safety requirements in the Enrolment Terms.
- Report concerns early.

Whānau/Parents/Caregivers

- Comply with responsibilities in the Enrolment Terms, including providing a safe and reliable device/connection and notifying CGA of security concerns.
- Support safe learning routines at home.
- Engage with CGA if online safety or wellbeing issues arise.

Prevention and Digital Wellbeing

CGA takes a prevention-first approach to online safety. The nature of digital technology — instant sharing, permanence, and reach beyond school platforms — means that harm can escalate quickly if it is not prevented early. For an online-only school, this makes prevention not just desirable but essential. CGA therefore prioritises proactive measures that reduce the likelihood of digital incidents occurring, and we make explicit links between prevention work and our incident response processes. Prevention strategies also help shift “digital bystander” culture by enabling students to recognise harm early, support peers, and seek help before issues intensify.

Effective prevention at CGA balances two complementary sets of strategies:

- **Promotional strategies** that build safe, responsible, and pro-social online behaviours (for example, teaching digital citizenship, relationship skills, and ethical participation online).
- **Protective strategies** that reduce or buffer risk through technical and procedural safeguards (for example, safe platform settings, monitoring, and clear reporting pathways).

Neither approach is sufficient on its own; prevention requires a deliberate and planned combination of both, reinforced over time.

CGA structures prevention using Netsafe's **Learn** – **Guide** – **Protect** model:

1. **Learn**: students develop competencies and values to keep themselves and others safe online as part of digital citizenship learning.
2. **Guide**: CGA's programmes and practices support student learning and strengthen a positive online culture — including curriculum integration, staff capability, and active partnerships with whānau.
3. **Protect**: CGA maintains technical and policy safeguards that underpin a safe digital environment, including clear reporting channels and platform safety controls.

Because students can access the internet from many different places and networks (home broadband, mobile data, public Wi-Fi), CGA's prevention work emphasises behaviour and safety skills, not just technical controls. We actively discuss with students how they use digital technology, the challenges they experience online, and practical ways to keep safe across all environments, not only within CGA platforms.

Prevention is also a whole-community effort. CGA involves students, parents/guardians, and whānau in meaningful discussions about how digital learning should work, what safe participation looks like, and how we respond when things go wrong. This shared approach helps:

- reinforce that online safety is a collective responsibility,
- support students to transition between home and school digital contexts,
- ensure cultural and social realities are reflected in our online practice, and
- normalise help-seeking and learning from mistakes.

CGA takes practical steps to prevent digital incidents by:

- embedding digital citizenship and online safety learning across the curriculum;
- teaching help-seeking and reporting skills, particularly for cyberbullying or unsafe content;

- configuring platforms with safety-by-design settings suited to an online-only school (e.g., moderated chat, controlled access, recording controls);
- training staff in safe online pedagogy and incident response;
- communicating expectations and supports to whānau/caregivers; and
- reviewing incidents and trends to continuously improve prevention.

CGA encourages students to use Netsafe's 🔗Children & Young People online safety hub for practical guidance on staying safe, managing risk, and getting support online.

Behaviour and Participation Expectations

Student behavioural expectations for online spaces are set out in detail in the Student Code of Conduct and the Enrolment Terms. This Online Safety Policy does not alter those expectations. Instead, it confirms that the expectations below apply in every CGA digital environment, including virtual classrooms, forums, group chats, email, collaborative documents, and any other space used for learning.

Because CGA is fully online, students move frequently between school platforms and wider online spaces. CGA encourages students to think deliberately about how their online behaviour and profiles reflect their values and affect others. This includes maintaining boundaries between personal and school use, and remembering that online conduct outside CGA platforms may still be addressed by CGA when it negatively impacts student wellbeing, relationships, or the learning environment.

Digital Citizenship / Online Safety

Students must:

- Protect passwords and never share login information.
- Only use CGA platforms for educational purposes.
- Report any cyberbullying, inappropriate content, or safety concerns immediately.
- Never share personal information (address, phone number) in public forums.
- Think before posting — would you say it face-to-face?

These expectations apply to all communication and participation connected to CGA, not only to live classes.

Respectful Communication

Students must:

- Use appropriate, respectful language in all online interactions.
- Be kind and constructive in feedback to peers.
- Not engage in bullying, harassment, or discriminatory behaviour of any kind.
- Respect others' opinions even when disagreeing.
- Not record, screenshot, photograph, or share class sessions or CGA learning materials without teacher permission and prior written permission where required.

These expectations help to protect the dignity, privacy, and safety of everyone in the online classroom.

Technology Use

Students must:

- Use school devices and platforms only for educational purposes during school time.
- Not game, use social media, or access entertainment during class time.
- Keep workspace and background appropriate for learning.
- Report technical issues promptly to their teacher.
- Use cameras and microphones only as directed by teachers.

These expectations help make CGA's virtual classrooms safe, focused, and inclusive for all learners.

Platform Use, Monitoring, and Recording

To safeguard students and maintain the integrity of CGA's online learning environment, CGA operates a controlled set of approved digital platforms. Students are required to access only authorised CGA systems and to use their own login credentials, consistent with the Student Code of Conduct and Enrolment Terms.

Because CGA is an online-only school, the use of CGA platforms may be monitored and recorded for safeguarding, quality assurance, and compliance purposes, as set out in the Enrolment Terms. Monitoring is undertaken lawfully and proportionately, in alignment with CGA's Privacy Policy and cybersecurity procedures. This monitoring may include activity logs, communications within CGA platforms, and recorded learning sessions/classes.

CGA may also use third-party cyber-safety tools to protect its systems and reduce risk, for example through filtering, threat detection, or moderated environments. These tools support prevention and early identification of unsafe behaviour or content.

Approved online services for teaching and learning

CGA will only require or recommend online services for learning where the school has reviewed the service's Terms & Conditions, including privacy, trust and safety provisions, and any licence or rights the provider asserts over uploaded content. CGA will not approve services whose data-sharing, advertising, or content-use practices are inconsistent with the Privacy Act 2020 or CGA's Privacy Policy. Where a platform has a minimum age requirement for account holders, CGA will ensure that the service is appropriate for the student cohort and that any required permissions or alternative arrangements are in place before the service is used for learning.

Students generally retain ownership of the original work they create through CGA learning activities. Where a specific service or learning task involves different conditions (for example a platform licence over content), CGA will make this clear to students and whānau in advance, and will only proceed where those conditions are suitable for school use.

Privacy in platform use

CGA explicitly teaches online privacy and safe participation. This includes helping students understand what constitutes personally identifying information, who can view shared content, how information may be stored or used now and in the future, and how to manage privacy settings appropriately for different learning contexts (for example sharing only within a class group versus sharing with whānau or publicly). CGA configures platform privacy settings to match the learning purpose and to keep student information appropriately protected.

Professional boundaries in online communication

Staff will not use personal or unapproved channels to teach or communicate with students. All staff–student online relationships must remain professional, learning-focused, and consistent with CGA's safeguarding standards. Communication occurs only through CGA-approved, recordable platforms, and staff do not connect with students through personal social media or private messaging.

Cybersecurity and Home Learning Environment

CGA recognises that students participate from a wide range of home environments and internet access points. Maintaining a safe online school therefore relies on both strong school-side protections and safe home-side practice.

Consistent with the Enrolment Terms:

- Parents/Guardians are responsible for ensuring students have safe and reliable access to an internet connection and device(s) meeting CGA's technical requirements.
- Parents/Guardians must maintain appropriate antivirus, firewall, and system updates, and use secure private networks (not public Wi-Fi) for CGA learning.
- Parents/Guardians must notify CGA immediately of any security concerns, data breaches, or unauthorised access.

CGA will take reasonable steps to maintain the integrity and security of its online systems, including applying security updates, access controls, monitoring and protective tooling, and safe platform configuration. However, CGA cannot guarantee uninterrupted access or protection from third-party risks beyond its control, such as outages or attacks on external services.

Shared approach to risk

Students access CGA learning through a variety of networks, including home broadband, mobile data, and community Wi-Fi. For that reason, CGA's approach to cybersecurity relies on active guidance and support as well as technical protections. CGA expects students and whānau to raise concerns early if they notice suspicious messages, unexpected account activity, scam attempts, or changes in device behaviour that could affect student safety.

Home learning wellbeing

A safe online learning environment includes attention to wellbeing and the practical realities of learning at home. CGA supports whānau to establish routines, physical setups, and boundaries that help students participate safely, respectfully, and without undue stress. Where learners face constraints such as shared devices, limited bandwidth, or challenging home circumstances, CGA will work with families to facilitate safe and equitable participation.

Generative AI and Emerging Technologies

CGA recognises that generative AI can support learning, creativity, and accessibility, but also introduces safety, privacy, and integrity risks. These tools can produce convincing but inaccurate answers, reflect hidden biases, and be misused to harm others. CGA's approach is to help students use AI confidently and critically, in ways that strengthen learning and protect wellbeing.

Students and staff must follow these expectations when using generative AI in connection with CGA learning:

- **Use AI only as permitted by teachers and CGA guidance.**

  Different tasks may allow different kinds of AI support. Teacher instructions for each activity are the rules to follow.

- **Treat AI output as a starting point, not a final authority.**

  Generative AI tools can produce made-up or incorrect information ("hallucinations") while sounding certain. Students must check important facts against reliable sources and use their own judgment before relying on AI content.

- **Look for bias, stereotypes, and cultural misrepresentation.**

  AI systems learn from human data, which can include unfair assumptions or gaps. Students should review AI-generated content for bias, missing perspectives, or inappropriate cultural use, and correct or reject it where needed.

- **Protect privacy and confidentiality.**

  Students and staff must not enter personal, sensitive, or CGA-confidential information into public AI systems. Information shared with some AI tools may be stored and could reappear in other people's results. If unsure whether something is safe to share, don't share it.

- **Maintain academic integrity.**

  Students must follow teacher instructions about acknowledging AI use and ensuring submitted work reflects their own understanding. AI may assist learning, but it must not replace genuine student thinking or be used to misrepresent authorship.

- **Do not use AI to harm or deceive.**

  AI must never be used to intimidate, humiliate, harass, or harm others, or to create misleading content such as deepfakes, impersonations, scams, or fabricated allegations.

- **Ask for help early.**

  If an AI tool produces disturbing content, seems to be encouraging unsafe behaviour, or is being used in a way that feels wrong, students should stop using it and talk to a teacher, Dean, counsellor, or the DSL. CGA may also recommend support through Netsafe.

Responding to Online Safety Incidents

What should be reported

Any member of the CGA community should report concerns including:

- Cyberbullying, harassment, hate speech, or discrimination.
- Threats of self-harm or harm to others.
- Sexualised content involving minors or grooming/exploitation.
- Privacy breaches, hacking, scams, impersonation, or unauthorised access.
- Unauthorised recording/sharing of CGA sessions or materials.
- Any behaviour making a student or staff member feel unsafe online.

CGA recognises that online incidents can involve a range of roles and relationships, including perpetrators, targets, and bystanders, and that these categories can overlap. We treat bystander behaviour as a key part of both prevention and response, because online harm often spreads or escalates through peer attention, forwarding, or silence.

CGA also acknowledges that harmful online behaviour may occur outside CGA platforms or outside class time. Where that conduct has, or could reasonably be expected to have, a negative impact on the safety, wellbeing, or educational functioning of CGA, the school has both responsibility and authority to respond. Our focus is on impact on the learning environment, not on when or where the conduct first occurred.

How to report

- Students: report to a teacher, Dean, counsellor, or directly to the DSL.
- Whānau/Caregivers: contact the DSL or Principal.
- Staff: report to the DSL as soon as practicable.

CGA encourages early reporting. Even where a person is unsure whether something “counts” as an incident, raising it quickly allows support and risk assessment before harm escalates. Reports can be made privately, and CGA will handle them discreetly and in line with privacy and safeguarding requirements.

Response process

CGA will respond to incidents in a way that is timely, proportionate, lawful, and centred on student safety. Prevention and response are linked: our response plan is designed to complement prevention work, and we use incidents to improve future prevention.

When an incident is reported, CGA will:

1. **Ensure immediate safety and wellbeing, including welfare checks where needed.**

   The first priority is to minimise distress or harm and maintain safety for all involved. This can include welfare checks, short-term learning adjustments, or safety planning for the affected student(s).

2. **Secure evidence appropriately and lawfully.**

   CGA will make a record of available information early (e.g., platform logs, timestamps, reported messages), recognising that online content may be deleted or altered. Staff will act to preserve the integrity of information and devices, and will seek specialist advice where needed.

3. **Assess severity, context, and those involved.**

   CGA will identify who is involved and how — recognising that targets and bystanders may also be perpetrators. We will look for links between online and offline behaviour, including whether the students involved know each other in person, and whether there are wider wellbeing or safety factors.

4. **Distinguish inappropriate conduct from unlawful conduct.**

   Many incidents can be addressed through CGA's behaviour, bullying, and safeguarding policies and processes. Where conduct appears criminal or otherwise unlawful, CGA will respond accordingly and involve appropriate external agencies.

5. **Act to stop harm and restore safety.**

   Actions may include platform controls, takedown requests, restorative steps, learning interventions, and/or discipline under relevant CGA policies. The focus is on stopping harm, supporting those affected, and preventing recurrence.

6. **Communicate with whānau where appropriate and lawful.**

   CGA will involve parents/guardians when it is necessary for safety, wellbeing, or resolution of the incident, and will do so in a way consistent with privacy requirements and the best interests of the learner.

7. **Escalate externally when required.**

   Depending on the incident, CGA may engage:

   - Netsafe for advice and support early in the response,
   - NZ Police where a crime may have occurred,
   - Oranga Tamariki / Ministry of Education where safeguarding thresholds are met, and
   - other relevant community supports where this helps restore safety and wellbeing.

   In certain circumstances, CGA may not be required to escalate a matter externally and instead will deal with it internally.

8. **Record, review, and improve prevention.**

   Incidents are logged and reviewed to identify patterns, platform risks, and learning needs, and to strengthen CGA's prevention work over time.

Important boundaries on account access: CGA will not access a student's private third-party accounts (e.g., personal social media) or require disclosure of passwords. Where account content is relevant to safety, CGA may ask a student to share information voluntarily in a way that does not amount to a "search" or require breaching platform terms.

Ownership considerations: CGA recognises that students generally own copyright in their original work, regardless of the device used. Device ownership (school-provided or BYOD) is handled under CGA's Enrolment Terms and relevant policies; response steps will reflect those ownership boundaries and legal protections.

Support

CGA will provide learning-focused and wellbeing support to those harmed and those who caused harm, aiming to restore safety and prevent recurrence. Support may include counselling, pastoral check-ins, restorative processes, safety planning, and guidance for whānau on how to reinforce safe online routines at home.

CGA may also recommend students access Netsafe's 🔗Children & Young People online safety hub for practical guidance and support.

Consequences and Access Restrictions

Consistent with the Enrolment Terms and the Student Learning, Wellbeing and Behaviour (Discipline and Safety) Policy, CGA responds to breaches of online safety expectations in ways that are proportionate, fair, and focused on restoring safety and learning. Responses may include restorative and educational steps, whānau engagement, and, where required, disciplinary action.

As an online-only school, CGA may use privacy-respecting safety and moderation tools within its platforms to prevent harm and maintain a safe learning environment. Where behaviour creates immediate risk, distress, or significant disruption, staff may take prompt online measures to stabilise the situation. These measures can include temporarily muting a student, removing a student from a live session, restricting chat functions, or suspending access to a specific platform while the matter is assessed. Such steps are protective in nature and are used to stop harm or prevent escalation.

Any temporary restriction will be followed by appropriate support and due process in line with CGA's behaviour and conduct processes. This includes clarifying what occurred, considering context and wellbeing factors, engaging whānau where appropriate, and determining next steps aimed at restoring a safe and inclusive learning environment.

Serious or repeated cyberbullying, harassment, discrimination, or other forms of digital harm may lead to longer-term restrictions, suspension, or withdrawal. Where conduct appears unlawful or

presents a significant safeguarding risk, CGA may refer the matter to Netsafe, Police, Oranga Tamariki, or other relevant agencies, including under the Harmful Digital Communications Act 2015.

Version Control

Policy No.:	CGA-SS-03
Approval Date:	19 March 2026
Previous Review Date:	N/A
Next Review Date:	19 March 2027

NB: This policy supersedes and replaces all prior policies and procedures relating to its subject matter, regardless of their date of approval.