



Brisbane State High School Generative Artificial Intelligence Policy (eSafety) 2026



Contents

1. Purpose	3
2. Scope	3
3. Guiding Principles	4
4. Approved and Responsible Use	4
5. Online Communications, Social Media and Student Images	5-6
6. Teaching, Learning and Assessment	7
7. Professional and Administrative Use	8
8. Roles and Responsibilities	8
9. Concerns, Incidents and Breaches	9
10. Capability, Implementation and Review	9
11. Definitions	10
12. Related Documents and Guidance	10

1. Purpose

1.1 This policy establishes the governance and minimum requirements for the safe, ethical, responsible and educationally purposeful use of generative artificial intelligence (genAI) at Brisbane State High School (BSHS).

1.2 It supports innovation while protecting student learning, assessment validity, privacy, security, wellbeing, equity, intellectual property and human accountability.

1.3 This policy sets the non-negotiable requirements. The linked BSHS Approach to genAI in Teaching, Learning and Assessment explains the school's pedagogical position and provides practical guidance for classroom and assessment decisions.

2. Scope

2.1 This policy applies to all staff, students, volunteers, contractors and other people using genAI for school-related work or learning, whether on or off school premises and whether using school or personal devices.

2.2 It applies to teaching, learning, assessment, administration, communications, co-curricular activities, planning and any other school function in which genAI is used.

2.3 This policy should be read with relevant Department of Education policies and procedures, the BSHS Learning Policy, Student Code of Conduct, ICT acceptable-use requirements, privacy and information-security requirements, copyright guidance and the BSHS Approach to genAI in Teaching, Learning and Assessment. [Insert links]



3. Guiding Principles

- 3.1** BSHS adopts a human-centred, thinking- and learning-first approach. GenAI may support people to think, learn, create and work, but it must not replace the human judgement, relationships, responsibility or productive effort central to education.
- 3.2** Use of genAI will be guided by the Australian Framework for Generative Artificial Intelligence in Schools and applicable Department of Education and QCAA requirements. Decisions will reflect the principles of teaching and learning, human and social wellbeing, transparency, fairness, accountability, and privacy, security and safety.
- 3.3** The educational purpose must determine whether and how genAI is used. Availability of a tool is not, by itself, a reason to use it.
- 3.4** A person remains accountable for decisions, advice, records, communications and work produced with genAI assistance. GenAI output must be critically reviewed and verified before use.

4. Approved and Responsible Use

- 4.1** Only Department- or school-approved genAI tools may be used with students or for school business. Use must comply with applicable age restrictions, parental consent requirements, procurement and risk-assessment processes, terms of use and approved purpose.
- 4.2** Users must not enter personal, sensitive, confidential, security-classified or commercially sensitive information into a genAI tool unless that tool and the specific use have been formally approved for that information.
- 4.3** Users must protect account credentials, follow cybersecurity requirements and report suspected privacy, security or safeguarding incidents through established school and Department processes.
- 4.4** Users must check outputs for accuracy, bias, fabricated information, harmful content, accessibility and appropriateness. Sources and intellectual property must be respected, and copyright or licensing requirements must be followed.
- 4.5** GenAI must not be used as the sole basis for a decision that materially affects a student, staff member or other person. Any consequential use requires an approved purpose, appropriate notice, meaningful human review and an accessible way to question or seek review of the decision.
- 4.6** GenAI-generated images, audio, video or representations of identifiable people must not be created or published without appropriate authority, consent and compliance with school and Department communication and media requirements. Deceptive impersonation, harmful synthetic media and non-consensual image manipulation are prohibited.

5. Online Communications, Social Media and Student Images

5.1 School-related social media, video-sharing and online collaboration may occur only through accounts, platforms and purposes authorised by the Department or school leadership. Personal social media accounts must not be used to communicate with students or to publish school content involving students.

5.2 Before an account or channel is established, the responsible area must document its purpose, intended audience, content and moderation arrangements, privacy and safety settings, administrators, recordkeeping requirements and review date. The platform must meet applicable age, consent, privacy, security and approved-use requirements.

5.3 Official accounts must use secure school-controlled credentials and multifactor authentication where available. At least two authorised staff members, including an appropriate leader or delegate, must have administrative access. Access must be reviewed when staff roles change, and accounts must be actively monitored.

5.4 Official social media is for approved school communication and community engagement. It is not the channel for complaints, disclosures or urgent safety concerns. Where commenting, messaging, tagging, sharing or remixing creates unnecessary risk, those functions should be restricted or disabled and users directed to established school contact and complaint pathways.

5.5 Content must be accurate, respectful, accessible, consistent with the school's values and branding, and must not disclose confidential information. Copyright, trademarks and the school's name, crest and other brand assets must be used only as authorised.

5.6 A student's personal information, image, voice, work or other identifying content may be captured or published only where the required consent is current and covers the particular purpose, audience, platform and form of publication. Consent records must be checked before publication. A student's or parent/carer's decision not to consent must be respected without disadvantage.

5.7 Student images or videos must not be published with the student's full name. Where naming is appropriate and consented, use a first name only, a first name with surname initial, or a non-identifying description such as year level, team or ensemble. Do not include student IDs, personal social media handles, date of birth, personal contact details, home location or other information that could unnecessarily identify or locate a student.

5.8 Images and captions must be considered together. Staff must avoid combinations of uniform, signage, location, timetable, event details, metadata or personal circumstances that create an avoidable safety or identification risk. Live location or travel information must not be posted where this may place a student or group at risk.

5.9 Images must preserve student dignity and reflect appropriate clothing, activity and context. Additional care is required where cultural considerations, disability, health information, child-protection concerns, custody or family violence circumstances, court orders or other vulnerabilities may increase risk. Where uncertainty exists, the image must not be published until advice is obtained.

5. Online Communications, Social Media and Student Images (Continued)

5.10 Student images and video must be created, transferred, stored, retained and deleted using approved school systems and devices. They must not be retained in personal photo libraries, personal cloud storage or personal messaging accounts. Unapproved copies should be deleted once the approved transfer or publication process is complete.

5.11 Staff must not tag student personal accounts, invite students to interact through staff personal accounts, or repost content from a student's personal account without appropriate authority and consent. Students must not be asked to create or maintain an age-restricted social media account for school learning or participation.

5.12 Student-created media intended for school publication requires staff review and the same consent, privacy, copyright, accessibility, safety and naming checks as staff-created content. Publication approval must be obtained through the school's established communications process.

5.13 AI-generated or AI-altered media must not imitate, replace or materially alter an identifiable student or staff member without explicit authority and appropriate consent. Synthetic content that could reasonably be mistaken for an authentic photograph, recording or statement must be clearly identified as AI-generated or AI-altered. Harmful, sexualised, humiliating or deceptive synthetic media is prohibited and must be reported immediately.

5.14 Requests or concerns about published images, personal information or online content must be taken seriously and acted on promptly. Content should be restricted or removed while privacy, safeguarding or consent concerns are assessed, where this is safe and practicable. Relevant evidence and records must be preserved in accordance with incident-response requirements.

5.15 AI-generated images, artwork, branding or designs must not be used on BSHS official public-facing communication channels. This includes the school's social media accounts, website, advertising, promotional materials and community publications. This applies regardless of whether the content is created or submitted by staff, students, contractors, parent groups, P&C subcommittees or other affiliated groups.

5.16 All content proposed for publication through official BSHS channels remains subject to school approval and must comply with BSHS branding, privacy, copyright, consent and communication requirements.

6. Teaching, Learning and Assessment

6.1 Teaching and learning use must support the intended learning and keep students intellectually active. Teachers determine when genAI adds educational value, when boundaries are required and when learning is best completed without genAI, consistent with the linked BSHS Teaching and Learning Approach to Generative AI.

6.2 Teachers must clearly communicate whether genAI use is prohibited or allowed for learning and assessment activities as per BSHS Teaching and Learning Approach to Generative AI. Within the context of digital learning BSHS uses two broad modes:

- Unplugged: the task or nominated components are completed without genAI so the student independently demonstrates the required knowledge, understanding, skills or thinking.
- Plugged In: genAI use is permitted, with the student remaining responsible for the thinking, decisions, verification, acknowledgement and final work.

6.3 Assessment must provide valid, authentic and sufficient evidence of what a student knows, understands and can do. Task design, process evidence, checkpoints and professional judgement are some of the primary safeguards; automated AI-detection results must not be treated as proof of misconduct or used as the sole basis for an adverse decision.

6.4 Where genAI use is permitted, students must follow the task conditions and acknowledge its use in the manner specified. Prompts, outputs, drafts or process evidence may be required.

6.5 Where authorship or authenticity is reasonably questioned, the school will use a fair evidence-based process. This may include discussion with the student, review of drafts and classwork, comparison with known work, or an opportunity for the student to demonstrate their knowledge and skills. Any academic-integrity response will follow the BSHS Learning Policy and relevant year-level, Department and QCAA processes.



7. Professional and Administrative Use

7.1 Staff may use approved genAI tools to support planning, drafting, analysis and administration where the use is appropriate, transparent when required, and consistent with professional obligations.

7.2 Staff must not outsource professional judgement or accountability to genAI. This includes decisions about assessment judgements including feedback, student support, behaviour, safety, staffing, recruitment, performance, legal obligations or other matters with significant impact.

7.3 Material produced with genAI must be checked by a suitably knowledgeable person before it is relied upon, shared or published. Public-facing content must also meet school branding, accessibility, media, privacy and approval requirements.

7.4 A new use, material change of purpose, integration or automation must be assessed through the relevant school and Department approval, privacy, information-security, procurement and risk processes before implementation.

8. Roles and Responsibilities

8.1 The Principal holds overall accountability for school risk and approves school-level implementation and exceptions within delegated authority.

8.2 The Deputy Principal responsible for Teaching and Learning and Digital Learning is the policy owner and coordinates implementation, advice, capability development, monitoring and review.

8.3 The school IT governance group provides advice on tool approval, risk, privacy, security, consent, records and emerging issues. It does not replace Department approval processes or the Principal's delegated authority.

8.4 The staff member or team responsible for school communications manages official accounts, publishing permissions, content approval, moderation, branding and removal or correction requests, in consultation with leadership and relevant student-safety staff.

8.5 Heads of Department and other leaders support consistent faculty and team implementation, including clear task conditions, appropriate authentication processes and escalation of concerns.

8.6 Teachers and staff comply with this policy, use approved tools and purposes, communicate expectations, protect information, verify outputs and retain responsibility for their professional work.

8.7 Students follow teacher directions and task conditions, use approved tools safely, protect personal information, acknowledge permitted use and ensure submitted work represents their own learning and contribution.

8.8 Parents and carers support students to understand and follow school expectations for safe, responsible and academically honest use.

9. Concerns, Incidents and Breaches

9.1 Concerns about unsafe, inappropriate or unauthorised genAI or online-media use must be reported through the existing school pathway appropriate to the issue, including teaching and learning, academic integrity, student wellbeing, behaviour, privacy, cybersecurity, child safety, complaints, communications or workplace conduct processes.

9.2 Responses will prioritise student safety and wellbeing, consider the student's views and circumstances, and be proportionate, procedurally fair and managed under applicable Department and school policy. A suspected student authenticity issue is not automatically a proven policy breach.

9.3 The school may need to respond when online conduct occurs outside school hours if it creates a reasonably foreseeable risk to safety or wellbeing, affects teaching and learning, or has a sufficient connection to the school. The response and any disciplinary action must remain within applicable Department and legal authority.

9.4 Privacy, image-based abuse, child-safety and security incidents must be escalated immediately through the relevant school and Department processes. Staff must know when matters require reporting to a platform, eSafety, police or another authority. Mandatory reporting, evidence preservation, recordkeeping and notification requirements continue to apply.

10. Capability, Implementation and Review

10.1 BSHS will progressively build staff and student capability to understand genAI and online safety, evaluate content, recognise risks, protect privacy, maintain authorship and make informed decisions about when and how to use genAI tools.

10.2 The school will consult staff, students and parents/carers as appropriate, including diverse and potentially vulnerable groups, when reviewing emerging online-safety issues and school expectations.

10.3 Relevant leaders and staff will maintain capability in responding to serious online incidents and in using platform, eSafety, police and Department reporting pathways where required.

10.4 Practical guidance, examples and tools may be updated more frequently than this policy. These supporting resources must remain consistent with this policy and the BSHS Approach.

10.5 This policy will be reviewed annually, or earlier when required by changes to legislation, Department or QCAA requirements, technology, evidence, risk or school practice.

11. Definitions

Approved genAI tool: A genAI tool approved for the relevant users, purpose, information and context through applicable Department and school processes.

Generative artificial intelligence (genAI): Artificial intelligence that generates content such as text, images, code, audio or video that resembles what humans can create.

Human review: Meaningful consideration by an appropriately authorised and knowledgeable person who can question, correct or reject a genAI-supported output or recommendation.

Personal or sensitive information: Information protected by applicable privacy, confidentiality, information-security or records-management requirements.

School: Brisbane State High School.

12. Related Documents and Guidance

- BSHS Approach to genAI in Teaching, Learning and Assessment [[link pending](#)]
- BSHS Learning Policy [[link](#)]
- BSHS Student Code of Conduct [[link](#)]
- Department of Education Digital and network use policy [[link](#)], privacy [[link](#)], information-security [[link](#)], acceptable-use [[link](#)], procurement [[link](#)], and generative-AI guidance [[link](#)]
- QCAA academic integrity, authentication and artificial-intelligence guidance [[link](#)]
- Australian Framework for Generative Artificial Intelligence in Schools [[link](#)]
- eSafety Commissioner, Toolkit for Schools – Prepare [[link](#)]
- eSafety, Checklist for developing effective online safety policies and procedures [[link](#)]
- eSafety, Guidelines for social media use, video sharing and online collaboration [[link](#)]
- eSafety, Tips for responding to incidents that happen outside school hours [[link](#)]

Generative Artificial Intelligence Policy (eSafety) 2026

Brisbane **State High** School

Address: Cnr Cordelia & Glenelg Streets, South Brisbane Qld 4101

Phone: (07) 3291 4111

Email: admin@brisbaneshs.eq.edu.au

Website: www.statehigh.com.au

