

# OECD AI Transparency Report

Organization: Fayston Preparatory School (KOR)

Reporting Period: Q2 2026

Published: October 2, 2026

## Section 0 – Your role in the AI system lifecycle

Responding as (please select all that apply):

- Deployer

If any of the fields above are selected, please indicate your organization size:

Medium-sized enterprise: 50-249 employees

## Section 1 – Risk Identification and Evaluation

### 1. How does your organization define and/or classify different types of risks related to AI?<sup>1</sup>

- Maintain an internal taxonomy, classification system, and/or set of risk area definitions
- Align with specific external frameworks, standards, reports, and/or guidance documents such as taxonomies, classification systems, and/or sets of definitions for risk areas (e.g. the NIST AI Risk Management Framework, the ISO/IEC 42001, the OECD AI Principles, the EU General-Purpose AI Code of Practice, the International AI Safety Report). (please specify): Fayston Preparatory School applies a risk-based approach to AI governance that classifies risks across educational, operational, governance, safeguarding, privacy, security, fairness, accountability, and institutional decision-making domains. Risk identification is informed by internationally recognized frameworks including the OECD AI Principles, Hiroshima AI Process Reporting Framework, NIST AI Risk Management Framework, ISO/IEC 42001, and emerging guidance related to advanced and agentic AI systems. Risk classifications are periodically informed by engagement with educators, researchers, accreditation organizations, policymakers, and international AI governance initiatives.
- Consult with external stakeholders (e.g., from academia, industry groups, civil society, or standard development organisations) when developing or updating risk taxonomies

**How does your organization define thresholds at which severe risks, unless adequately mitigated, may be considered "unreasonable"? Please describe the framework(s) most relevant to your organization's role and context. If your organisation does not use formal thresholds, you may describe instead the policies, decision criteria, or governance processes you apply when assessing severe AI risks. You may also describe:**

- Specific examples of contexts in which your models or systems could, in your assessment, pose unreasonable or intolerable risk;
- How mitigations are graduated by capability or propensity level;
- How your organisation considers the specificities of different AI technologies, such

**as generative AI and agentic AI, including any specific risk assessment or governance mechanisms applied to agentic AI capabilities.**

Fayston does not use a single quantitative threshold for determining unacceptable AI risk. Instead, risks are evaluated according to the potential impact of AI-assisted outputs on individuals, institutional operations, educational outcomes, legal obligations, safeguarding responsibilities, and organizational accountability.

Higher-risk use cases require increased levels of verification, human oversight, documentation, and authorization. AI-generated outputs may inform decisions but are not independently authorized to determine consequential actions involving student welfare, safeguarding, disciplinary measures, employment decisions, accreditation matters, or institutional governance.

As AI systems become increasingly capable and autonomous, Fayston places particular emphasis on preserving meaningful human judgment, preventing inappropriate reliance on AI-generated outputs, and maintaining clear accountability for consequential decisions. Emerging agentic AI capabilities are evaluated according to their level of autonomy, potential for independent action, and ability to affect institutional processes without adequate human review.

## **2. Both before and after deployment, what practices does your organization use to identify and evaluate vulnerabilities, incidents, emerging risks and misuse throughout the AI system lifecycle?**

- Publicly available benchmarks and measurement tools
- Qualitative assessments (e.g., expert judgment, narrative scoring)
- Impact assessments such as personal data protection assessment and fundamental rights impact assessments
- Specific risk identification practices for vulnerable groups
- Internal model, system, or application-independent research initiatives
- External model, system, or application-independent research initiatives
- Vulnerability reports
- Incident reports, including reports shared by other organizations
- Specific risk identification practices for agentic AI capabilities, e.g., autonomous action-taking, tool use, multi-step planning (please specify): Fayston evaluates potential risks associated with AI systems that may demonstrate agentic characteristics, including autonomous action recommendations, tool use, multi-step task execution, workflow automation, and delegated decision support. Risk identification focuses on human oversight requirements, verification of outputs, escalation pathways, accountability for consequential decisions, privacy implications, and the appropriateness of AI use within educational settings. The institution emphasizes human review and authorization before actions affecting students, staff, or institutional operations are taken.
- Multilingual and cross-cultural evaluation, including collaboration with local ecosystems (e.g., national AI institutes, language-specific evaluation consortia) for under-represented languages and cultural contexts (please specify): Fayston operates in a multilingual and multicultural educational environment serving students, families, and staff from diverse linguistic and cultural backgrounds. Evaluation activities consider differences in language, cultural context, interpretation, communication norms, and educational expectations. The institution draws upon international educational frameworks, global accreditation

practices, and participation in international governance and policy discussions to identify potential cultural, linguistic, and contextual risks associated with AI-generated outputs.

- Assessment of risks arising from interactions among multiple AI agents

**How does your organization monitor the interactions of AI agents under your control with other agents / assess risk from multiple agents interacting?**

Fayston does not deploy autonomous multi-agent AI systems in operational educational environments. Where multiple AI tools may be used together within workflows, risks are assessed through human oversight, output verification, review of information consistency, and evaluation of potential impacts on decision-making. The institution focuses on identifying risks related to compounding errors, conflicting recommendations, overreliance on AI-generated outputs, and reduced human accountability. Human review remains required for consequential decisions involving students, staff, academic programs, or institutional operations.

**Please briefly describe your organization's decision-making process for deploying an AI model or system including: who has decision authority; what evidence and criteria are required (e.g., performance, safety/security, robustness, fairness, privacy, compliance, independent external testing, evaluation, validation and verification (TEVV) or assurance); contextual caveats or limitations required in interpreting risk evaluation metric results; what approvals/sign-offs are needed; and what safeguards (e.g., mitigations, monitoring, or phased release) must be in place to move into deployment.**

Decisions regarding deployment of AI systems are made by institutional leadership and relevant administrative personnel based on educational value, safety, privacy considerations, legal compliance, operational suitability, and alignment with institutional objectives.

Prior to adoption, AI systems may be evaluated through pilot use, educator feedback, review of vendor documentation, publicly available evaluations, security and privacy considerations, and assessment of potential impacts on students, faculty, and institutional processes.

Higher-risk applications require increased scrutiny, human oversight, verification procedures, and governance controls. AI-generated outputs are treated as decision-support inputs rather than decision authorities. Human decision-makers remain responsible for interpretation, verification, authorization, and accountability for consequential decisions.

**Following deployment, how do you use incident reports — including those shared by other organizations — to identify emerging issues, update risk assessments, and trigger corrective actions.**

Fayston monitors developments related to AI safety, reliability, security, misuse, and governance through vendor communications, public incident reporting, research publications, professional networks, and participation in international AI governance initiatives. Relevant incidents are reviewed to assess applicability to educational and institutional contexts.

Lessons learned from internal observations and external incident reports may inform updates to guidance, risk assessments, staff awareness activities, governance controls, and deployment practices. Where necessary, corrective actions may include additional oversight requirements, restrictions on use cases, revised procedures, or suspension of specific applications.

**3. Does your organization have mechanisms to receive and/or share reports of risks, incidents or vulnerabilities by/with third parties?**

Yes, receiving only

**If yes, please indicate which stakeholders reporting mechanisms may be accessible to, recognising specifics will depend on the nature of the report and risk level. For each, indicate whether access is on a standing basis (Always), activated based on context (Ad hoc/as relevant), or not currently accessible.**

|                                                                                             | Always | Ad hoc / as relevant     | Not currently accessible |
|---------------------------------------------------------------------------------------------|--------|--------------------------|--------------------------|
| Relevant employees (security, legal/compliance, etc.)                                       |        |                          |                          |
| Public authorities (e.g., public reporting offices for security incidents or data breaches) |        | <input type="checkbox"/> |                          |
| Supervisory authorities (e.g., data protection authorities)                                 |        | <input type="checkbox"/> |                          |
| Industry partners or industry fora                                                          |        | <input type="checkbox"/> |                          |
| Users (end users, enterprise customers, developers using APIs)                              |        | <input type="checkbox"/> |                          |
| Business customers / deploying organizations (if different from “users”)                    |        |                          |                          |
| Supply-chain partners (cloud, data providers, etc.)                                         |        |                          |                          |
| Academia / researchers                                                                      |        | <input type="checkbox"/> |                          |
| Independent auditors                                                                        |        |                          |                          |
| Standards bodies / multi-stakeholder initiatives (OECD.AI, ISO/IEC, IEEE, etc.)             |        | <input type="checkbox"/> |                          |
| Specific civil society organizations                                                        |        |                          |                          |
| Media / general public (people or communities indirectly impacted)                          |        |                          |                          |
| Other                                                                                       |        |                          |                          |

**Please describe how your organisation determines when and how reporting mechanisms are made accessible to different stakeholders (e.g. based on legal or regulatory requirements, internal policies, or risk level). Please also provide public URLs or details on how to submit reports. If none, write “Not applicable”**

Fayston determines the accessibility of reporting mechanisms based on the nature of the issue, applicable legal and regulatory requirements, institutional policies, privacy obligations, and the potential impact on students, staff, families, and school operations.

Internal reporting channels are available to relevant employees responsible for leadership, technology, compliance, safeguarding, privacy, and risk management. Where appropriate, information may be shared with educational stakeholders, accreditation organizations, public authorities, professional associations, researchers, or multi-stakeholder governance initiatives.

As an educational institution deploying third-party AI systems rather than developing frontier AI models, Fayston primarily receives risk, incident, vulnerability, and governance information from technology providers, professional networks, accreditation organizations, standards bodies, and international governance initiatives. Reporting and information-sharing practices are conducted on a need-to-know basis and are subject to applicable privacy, confidentiality, safeguarding, and institutional governance requirements.

Reports may be submitted through established institutional communication channels, including administrative reporting processes, technology support channels, leadership review processes, and applicable vendor reporting mechanisms.

**4. If your organization has programs to incentivize risk(s) disclosure, incidents and systemic vulnerabilities, please share what type of programs you use?**

- Internal incentives and culture

**Please provide public URLs and/or details on your incentive program(s). If none, write “Not applicable.”**

Fayston does not maintain formal bug bounty programs, vulnerability disclosure reward programs, or financial incentives related to AI risk reporting. As an educational institution deploying third-party AI systems, the institution promotes responsible risk identification, incident reporting, and governance awareness through professional expectations, leadership guidance, staff training, and a culture of accountability.

Faculty, staff, and administrators are encouraged to raise concerns regarding AI use, privacy, security, academic integrity, misinformation, bias, safeguarding, or other governance-related risks through established institutional reporting channels. Reports are reviewed through existing leadership, compliance, technology, safeguarding, and governance processes.

The institution's approach emphasizes transparency, responsible use, continuous improvement, and shared responsibility rather than formal incentive or reward programs.

**5. Does your organization use or contribute to the development of international technical standards, best practices or tools for the identification, assessment, and evaluation of risks?**

Contributes and uses

**If contributes or uses, please select all that apply:**

- NIST AI Risk Management Framework (AI RMF)
- Industry-led best practices or codes of conduct
- OECD Due Diligence Guidance for Responsible AI
- Other international or regional standards (please specify): OECD AI Principles; Hiroshima AI Process (HAIP) Reporting Framework; UNESCO Recommendation on the Ethics of Artificial Intelligence; ACSI and MSA institutional governance standards; applicable South Korean privacy and education regulations.

**6. Does your organization collaborate with relevant stakeholders across sectors to assess and adopt risk mitigation measures to address risks that could have broad and potentially cascading socio-**

**economic impacts? Please indicate which stakeholders you collaborate with, and whether collaboration is on a standing basis (Always-on), activated based on context (Ad hoc/as relevant), or there is no current collaboration.**

|                                                                                                                                                                      | Always-on                | Ad hoc / as relevant     | No current collaboration |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|--------------------------|--------------------------|
| Relevant employees (security, legal/compliance, etc.)                                                                                                                | <input type="checkbox"/> |                          |                          |
| Public authorities / regulators / AI safety institutes / other public sector bodies and inter-governmental coordination structures                                   | <input type="checkbox"/> |                          |                          |
| Industry partners or industry fora                                                                                                                                   |                          | <input type="checkbox"/> |                          |
| Users (end users, enterprise customers, developers using APIs)                                                                                                       |                          |                          |                          |
| Business customers / deploying organizations (if different from “users”)                                                                                             |                          |                          |                          |
| Supply-chain partners (cloud, data providers, etc.)                                                                                                                  |                          |                          |                          |
| Academia / researchers                                                                                                                                               | <input type="checkbox"/> |                          |                          |
| Independent auditors                                                                                                                                                 |                          | <input type="checkbox"/> |                          |
| Standards bodies / multi-stakeholder initiatives (OECD.AI; ISO/IEC; IEEE; AIID etc.)                                                                                 | <input type="checkbox"/> |                          |                          |
| Independent civil society organizations (e.g., for evaluations, audits, or policy review)                                                                            |                          | <input type="checkbox"/> |                          |
| Media / general public (people or communities indirectly impacted)                                                                                                   |                          | <input type="checkbox"/> |                          |
| Other(s) (please add any other relevant stakeholder groups)::<br><i>Accreditation organizations, educational institutions, and international governance networks</i> |                          | <input type="checkbox"/> |                          |
| Not applicable                                                                                                                                                       | <input type="checkbox"/> |                          |                          |

**Please describe examples of how your organization collaborates. Examples may include: participating in multi-stakeholder or industry initiatives; partnering with academia, civil society, or the public sector; establishing internal or joint governance structures with external experts or in partnership with other efforts to share knowledge and jointly address risks.**

Fayston collaborates with stakeholders across education, accreditation, research, policy, and international AI governance communities to identify emerging risks and promote responsible AI deployment. The institution participates in international initiatives including the OECD/G7 Hiroshima AI Process and engages with researchers, educators, accreditation organizations, standards communities, and governance practitioners to exchange knowledge and improve implementation practices.

Collaboration activities include participation in interoperability initiatives, governance discussions, professional development efforts, capacity-building activities, and knowledge-sharing related to AI governance, accountability, transparency, and human oversight. These engagements help inform institutional policies, risk management practices, and responsible deployment approaches in educational settings.

**Any further comments and implementation documentation.**

*No answer provided*

## Section 2 – Risk Management and Information Security

**7. Across the AI system lifecycle, what steps does your organization take to manage risks and vulnerabilities? Please indicate which specific practices, tools or metrics your organization uses at each lifecycle stage. You may refer to tools or metrics present in the OECD.AI Catalogue of Tools and Metrics or suggest additions. Respondents may complete only the lifecycle stages relevant to their organisation's role. Stages that do not apply may be left blank.**

**Plan and design**

**Collect and process data**

**Build, integrate and interpret model**

**Verify and validate**

**Deploy**

**Operate and monitor**

**Please provide a consolidated description of your organisation's approach to risk management across the AI system lifecycle, including how the practices identified above operate together and any cross-cutting governance, review or escalation processes. Please also indicate how often these practices are reviewed and what types of events trigger reviews and updates. Where relevant, please distinguish between different types of AI systems (e.g. generative or agentic AI).**

Fayston applies a risk-based approach to AI governance throughout the AI system lifecycle. Prior to adoption, AI systems are evaluated for educational value, privacy implications, security considerations, legal compliance, operational suitability, and potential impacts on students, staff, and institutional decision-making. Higher-risk use cases require increased levels of verification, oversight, documentation, and authorization.

Risk management practices continue following deployment through monitoring of emerging guidance, vendor communications, incident reports, governance developments, and institutional observations. Significant incidents, capability changes, or emerging risks may trigger review of existing practices, additional safeguards, updated guidance, or restrictions on use.

Across all AI use cases, Fayston emphasizes accountability, human oversight, transparency, and preservation of meaningful human judgment. AI-generated outputs are treated as decision-support

inputs rather than decision authorities, particularly in consequential educational, safeguarding, employment, or governance contexts.

**Please describe any measures used to ensure data quality and fairness across the data collection and curation stage (e.g., dataset audits, filtering training data to remove harmful content or personal information, fine-tuning on curated data, use of moderation tools, assessment of limitations to model generalisability).**

Fayston does not develop or train foundation AI models. When evaluating and deploying AI systems, the institution considers available information regarding model limitations, bias, fairness, reliability, privacy protections, and intended use cases. Particular attention is given to educational contexts, vulnerable populations, multilingual use, and potential impacts on student outcomes.

Users are encouraged to verify AI-generated outputs, consider contextual limitations, and apply professional judgment when interpreting recommendations or generated content. Higher-risk uses require increased human review and verification before consequential actions are taken.

## **8. What security measures are used in testing AI systems?**

- Human-in-the-loop controls for higher-risk test cases
- Access controls, including roles-based permissions
- Audit logging and monitoring

**8.A. Please indicate, if relevant, the team or role responsible for overseeing secure testing and whether this responsibility is shared across multiple teams and/or functions.**

Responsibility for AI evaluation, governance, and secure deployment is shared across school leadership, technology personnel, academic administrators, and other relevant institutional stakeholders. Reviews are conducted in accordance with existing privacy, safeguarding, compliance, accreditation, and operational governance processes.

Because Fayston primarily deploys third-party AI systems rather than developing AI models, testing activities focus on evaluating educational suitability, privacy implications, operational risks, user access controls, and governance considerations. Higher-risk use cases receive increased human review, documentation, verification, and approval before implementation.

Significant concerns, incidents, or identified risks may be escalated to senior leadership for additional review and decision-making.

## **9. How does your organization protect intellectual property, including copyright-protected content?**

**9.A. Safeguards that promote lawful data use and transparency in AI training:**

- Maintain a copyright policy that addresses data sourcing, content provenance, safeguards, and organizational roles and responsibilities
- Other(s) (please specify): Academic integrity requirements, attribution expectations, responsible AI use guidance, and review of vendor copyright and intellectual property terms prior to adoption.

**9.B. Safeguards that reduce the risk of dissemination of outputs that may infringe copyright:**

- Designating clear points of contact so creators or rights holders can raise concerns about infringing outputs
- Restricting outputs that raise ethical, human rights, or legal concerns—such as non-consensual intimate imagery, unauthorized deepfakes, or outputs that are substantially similar to copyrighted works.

## **10. How do you protect privacy and prevent your systems from disclosing confidential or sensitive data across the AI lifecycle?**

- Make information about data privacy, practices, and controls accessible to a diverse set of stakeholders
- Use security controls, including encryption at rest and in transit

### **Describe key privacy measures and data-protection standards applied.**

Fayston protects personal information through institutional privacy practices, access controls, secure technology platforms, vendor review processes, and staff expectations regarding responsible data handling. The institution seeks to minimize unnecessary disclosure of personal information when using AI-enabled systems and encourages use of privacy-protective configurations where available. Staff and students are instructed not to submit sensitive personal information into AI systems unless appropriate safeguards, permissions, and institutional requirements have been satisfied. Privacy considerations are incorporated into evaluation, selection, and deployment decisions involving AI-enabled technologies.

## **11. How does your organization assess cybersecurity risks and implement policies to enhance the cybersecurity of advanced AI systems across the AI system lifecycle? Respondents may complete the checkbox subsections in 11.A–11.D or describe their overall approach under 11.E.**

### **11.A. Governance, policy and assessments**

- Maintain or update security policies aligned with recognized standards (e.g., NIST CSF, ISO/IEC 27001, SOC 2, CIS Critical Security Controls), and review them regularly in response to emerging risks or regulatory guidance
- Implement incident response, disaster recovery, or business continuity plans, including escalation procedures for high-severity incidents
- Train staff on cybersecurity best practices and AI-specific threats, including how to recognize and respond to misuse or unintended outcomes of advanced AI systems
- Integrate cybersecurity AI risks into broader cybersecurity risk management activities
- Regularly review security measures and update them in response to emerging risks, incidents, or major releases
- These responsibilities are delegated contractually to model or infrastructure providers

### **11.B. Technical and operational controls**

- Apply multi-factor authentication (MFA) and role-based access controls for advanced AI systems
- Conduct secure AI development and/or deployment practices
- These responsibilities are delegated contractually to model or infrastructure providers

- Monitor system activity and log access to detect anomalies or misuse

#### **11.C. Protection of sensitive or high value AI assets**

- Limit access to proprietary AI assets based on role or need-to-know
- Require NDAs or confidentiality agreements for staff and contractors with access
- These responsibilities are delegated contractually to model or infrastructure providers

#### **11.D. Insider risk protection detections**

- Conduct pre-employment screening or role-sensitive vetting
- Provide staff training on cybersecurity best practices and AI-specific threats
- Implement insider-risk escalation or response procedures
- Monitor for unauthorized internal access or suspicious activity

#### **11.E. Please describe the main security measures your organization applies and indicate which are specific to particularly sensitive AI assets, where relevant.**

Fayston's security approach combines institutional cybersecurity practices, role-based access controls, privacy protections, staff training, vendor due diligence, and established incident response processes. The institution relies on reputable technology providers that maintain security certifications, encryption controls, infrastructure protections, and operational security practices while maintaining local governance controls regarding access, authorization, and responsible use.

Security considerations are incorporated into AI evaluation and deployment decisions. Particular attention is given to protection of student information, educational records, safeguarding-related information, and other sensitive institutional data. Staff are expected to follow institutional policies governing confidentiality, acceptable use, and responsible handling of AI-enabled technologies.

### **12. What is your organization's vulnerability management process? Does your organization take actions to address identified risks and vulnerabilities, including in collaboration with other stakeholders?**

- Investigation of reported or identified risks and vulnerabilities
- Defined escalation criteria and follow-on actions for identified vulnerabilities (e.g., for external reporting or information sharing)
- Reporting to regulators / authorities when relevant

### **13. What post-deployment practices does your organization use to monitor and respond to vulnerabilities, incidents, emerging risks and misuse of advanced AI systems?**

- Conduct post-deployment monitoring
- Perform root-cause analysis and apply lessons learned to improve future development and/or deployment practices

### **14. Do you develop or deploy agentic AI systems (systems that can autonomously plan/act or use tools)?<sup>4</sup>**

No

**Please provide any further comments and implementation documentation.**

Fayston recognizes that advances in generative and agentic AI create both opportunities and governance challenges. The institution's approach emphasizes responsible deployment, meaningful human oversight, accountability, privacy protection, cybersecurity, and preservation of human judgment in consequential decisions.

Through participation in international initiatives including the OECD/G7 Hiroshima AI Process, interoperability efforts, and AI governance capacity-building activities, Fayston seeks to contribute practical implementation perspectives from the education sector while supporting trustworthy and human-centered AI adoption.

### Section 3 – Transparency Reporting on Advanced AI Systems

**15. Does your organization publish public reports and/or technical documentation related to the capabilities, limitations, and domains of appropriate and inappropriate use of advanced AI systems? Are these clear and understandable by non-technical audiences?**

Yes

**15.A. If yes, which of the following information is included in your organization's publicly available documentation for any of your AI products?**

- Capabilities, behaviours, and limitations, including domains of appropriate and inappropriate use or indicative thresholds associated with systemic risks.
- Technical documentation and instructions for use if relevant.
- Plain-language or non-technical summaries
- Other (specify): AI governance guidance, responsible-use expectations, academic integrity requirements, human oversight requirements, and educational AI literacy resources.

**Please provide links or references showing where this information is made public.**

*No answer provided*

**15.B. If yes, how often are such reports usually updated?**

Other (e.g., triggered by material changes, incidents, or new risks)

**16. How does your organization share information with a diverse set of stakeholders (other organizations, governments, civil society and academia, etc.) regarding the outcome of evaluations of risks and impacts related to an advanced AI system?**

- Public documentation
- Direct engagement with AI safety institutes, civil society or academic partners
- Other (specify): International AI governance initiatives and standards communities

**Describe how evaluation results are shared and with which stakeholders (e.g. other organizations, governments, civil society and academia, etc). You may also indicate whether non-technical or plain-language summaries are provided for broader audiences.**

Fayston shares information regarding AI use, governance, risks, limitations, and responsible deployment practices through institutional communications, professional development activities, governance discussions, and stakeholder engagement. Information is communicated to educators, students, families, accreditation organizations, and professional networks using language appropriate to the intended audience.

The institution also participates in international AI governance discussions and knowledge-sharing initiatives involving educational organizations, researchers, standards communities, accreditation bodies, and public-interest stakeholders. Where appropriate, information is shared in accessible, non-technical formats that support understanding of both opportunities and limitations associated with AI-enabled systems.

**17. Does your organization publish public privacy policies addressing the use of personal data, user prompts, and/or the outputs of advanced AI systems?**

Yes

**If yes, provide links to privacy policies or notices covering personal data, user inputs, and AI-generated outputs.**

Fayston maintains privacy notices and institutional policies governing the collection, use, storage, and protection of personal information. When AI-enabled tools are used, applicable privacy requirements, vendor terms, student protection requirements, and institutional policies continue to apply. The institution evaluates AI tools for privacy, security, educational suitability, and compliance considerations prior to adoption.

Relevant privacy information is made available through institutional policies, enrollment documentation, technology-use guidance, and applicable notices provided to students, families, faculty, and staff.

**18. How does your organization provide information about the sources of data used for the training of advanced AI systems, as appropriate, including information related to the sourcing of data annotation and enrichment?**

- Not applicable

**Please provide links to any publicly available information.**

Not applicable. Fayston does not develop or train advanced AI models and therefore does not maintain training-data documentation.

**19. Does your organization demonstrate transparency related to advanced AI systems through any other methods?**

Yes

**If yes, describe additional method(s), including where relevant transparency measures related to AI agents**

Fayston promotes transparency regarding AI use through responsible-use guidance, academic integrity expectations, professional development activities, governance discussions, parent and student communications, and AI literacy initiatives. Information is provided regarding the benefits, limitations, risks, and appropriate use of AI-enabled systems in educational settings.

The institution emphasizes disclosure when AI tools are used in learning activities, preservation of meaningful human oversight, verification of AI-generated outputs, and accountability for consequential decisions. Fayston also contributes to broader AI governance discussions through participation in international, accreditation, and professional communities.

**20. Does your organization publish statistical insights derived from anonymised, aggregated usage data to advance understanding of AI adoption and its economic impacts in areas including occupations and tasks by region, sector and country? To this end, do you contribute to international cooperation efforts?**

No

**Please estimate the total staff time and annual expenses associated with conducting compliance activities and include any further comments and implementation documentation (optional).**

AI governance and compliance activities are integrated into existing leadership, technology, privacy, safeguarding, accreditation, and institutional governance processes. Activities include policy review, staff guidance, stakeholder communication, vendor evaluation, risk assessment, professional development, monitoring of emerging AI governance developments, and participation in international governance initiatives. Because Fayston functions primarily as an educational institution deploying third-party AI systems rather than developing foundation models, compliance activities are generally proportional to operational use, educational impact, privacy considerations, and institutional risk exposure.

## **Section 4 – Organizational Governance, Incident Management, and Transparency**

**21. How has AI risk management been embedded in your organization's governance framework?**

- Executive oversight
- Senior management oversight
- Governance council or committee
- Other (e.g., distributed / multi-institutional governance arrangement) (please specify): Fayston participates in multi-stakeholder and multi-institutional AI governance activities through accreditation organizations, international AI governance initiatives, professional networks, standards discussions, and educational collaborations. These engagements inform institutional governance practices while decision-making authority remains with designated school leadership.

**Please describe how AI risk management is integrated into governance structures, including: which roles or bodies have advisory versus decision-making authority; which roles or bodies have final accountability for AI risk-related decisions; and how often policies are reviewed or updated (e.g., following major incidents, regulatory changes, or material updates to systems).**

AI governance is integrated into existing institutional governance, leadership, compliance, safeguarding, accreditation, and risk-management structures. Oversight is exercised through executive leadership and senior management processes responsible for technology adoption, educational quality, student welfare, privacy, compliance, and organizational accountability.

Decisions regarding the adoption and use of AI-enabled systems are evaluated according to intended use, educational impact, privacy considerations, operational risk, and the level of human oversight required. Higher-risk uses require additional review, verification, and human decision-making authority before implementation.

Final accountability for consequential decisions remains with designated institutional leaders rather than AI systems. AI-generated outputs may inform decision-making but do not replace human responsibility, professional judgment, or institutional accountability.

Policies and practices are reviewed periodically and may be updated in response to changes in technology, emerging governance guidance, regulatory developments, accreditation expectations, stakeholder concerns, or lessons learned from implementation.

## **22. Are relevant staff trained on your organization's governance policies and risk management practices?**

Yes

**If yes, describe training methods (e.g., onboarding modules, regular sessions, and confidential channels to report concerns).**

Relevant staff receive guidance and professional learning regarding responsible AI use, academic integrity, privacy considerations, human oversight, verification practices, student protection, and institutional accountability. Training is delivered through professional development sessions, leadership communications, policy guidance, collaborative discussions, and ongoing support activities.

Staff are encouraged to report concerns through established leadership, safeguarding, technology support, compliance, and administrative channels. Emerging AI-related risks, incidents, or policy developments may prompt additional training, review, or guidance.

## **23. Are steps taken to address reported incidents documented and maintained internally?**

Yes

**If yes, describe how incident records are kept and used for follow-up (e.g., incident logs, root-cause analysis reports, internal tracking systems). You may indicate whether and how you define escalation thresholds for when incidents must be surfaced to senior leadership or external parties.**

AI-related concerns, incidents, or governance issues are documented through existing institutional reporting, safeguarding, compliance, technology support, and administrative review processes. Records are maintained to support follow-up actions, lessons learned, policy refinement, and risk mitigation activities.

Incidents involving privacy, security, safeguarding, legal compliance, significant operational impact, or consequential decision-making are escalated to appropriate leadership for review. Depending on the nature of the issue, additional investigation, vendor engagement, corrective actions, or policy updates may be undertaken.

**24. Does your organization share research and best practices on addressing or managing risk?**

Yes

**If yes, describe how research or good practices are shared (e.g., publications, conferences, collaborations with other sectors).**

Fayston shares AI governance and responsible-use practices through professional presentations, accreditation activities, international AI governance initiatives, publications, working groups, conferences, and cross-sector collaborations. The institution contributes practical perspectives from educational implementation, governance, oversight, and institutional decision-making.

Participation in international initiatives, accreditation communities, professional networks, and research activities supports the exchange of lessons learned regarding AI governance, human oversight, accountability, transparency, and responsible deployment practices.

**25. Does your organization use international technical standards or best practices for AI risk management and governance policies?**

Yes

**If yes, please indicate which standards or frameworks apply:**

- ISO/IEC standards (e.g., ISO/IEC 27001, ISO/IEC 42001)
- NIST AI Risk Management Framework (AI RMF)
- OECD AI Principles
- Other international or regional standards (please specify): OECD Hiroshima AI Process (HAIP); Accreditation governance frameworks; Responsible AI governance and assurance frameworks.
- Industry-led best practices or codes of conduct

**If yes, describe which international technical standards or best practices your organization uses.**

Fayston's AI governance approach is informed by internationally recognized frameworks and best practices, including the OECD AI Principles, OECD Hiroshima AI Process (HAIP), NIST AI Risk Management Framework (AI RMF), relevant ISO/IEC standards, accreditation expectations, and responsible AI governance practices.

These frameworks support institutional approaches to transparency, accountability, human oversight, risk assessment, privacy protection, educational suitability, and responsible deployment. Frameworks are adapted to the educational context and applied proportionally according to the nature, purpose, and potential impact of AI-enabled systems.

**Any further comments and implementation documentation.**

Fayston recognizes that advances in generative and agentic AI create both opportunities and governance challenges. The institution's approach emphasizes responsible deployment, meaningful human oversight, accountability, privacy protection, educational benefit, and proportional risk management. As an educational institution deploying third-party AI systems rather than developing foundation models, Fayston focuses on governance, operational oversight, transparency, verification, safeguarding, and institutional accountability throughout the AI system lifecycle. The institution draws upon internationally recognized frameworks and participates in global AI governance discussions to support continuous improvement and responsible implementation practices. Fayston remains committed to ensuring that AI supports human learning, professional judgment, student well-being, and institutional trust.

## Section 5 – Content Authentication & Provenance Mechanisms

**26. What mechanisms, if any, does your organization put in place to allow end-users, where possible and appropriate, to know when they are interacting with an advanced AI system developed by your organization?**

- User disclosure (e.g., text notice, verbal statement, or system label)
- Documentation or FAQs explaining when and how AI is used in the system
- Distinct branding or labeling for AI-generated content (e.g., “AI-generated” tag, metadata label)

**Provide any additional details or context on how or when users are informed they are interacting with advanced AI systems (e.g. if such mechanisms are planned, in testing, or applied only to certain products).**

Fayston promotes transparency regarding the use of AI tools through institutional guidance, professional development, classroom expectations, and responsible-use policies. Students, educators, and staff are encouraged to disclose the use of AI tools when appropriate and to distinguish AI-assisted work from independently produced work.

Information regarding AI use is communicated through guidance documents, training activities, classroom discussions, and institutional communications. The institution emphasizes transparency, responsible use, academic integrity, and human accountability when AI tools are used in educational settings.

Because Fayston primarily deploys third-party AI applications rather than developing proprietary AI systems, transparency mechanisms are generally implemented through policy, disclosure expectations, and educational practices rather than technical watermarking solutions.

**27. Does your organization use content provenance detection, labeling or watermarking mechanisms that enable users to identify content generated by advanced AI systems?**

No

**Any further comments and implementation documentation.**

Fayston recognizes the importance of content authenticity, transparency, and provenance in AI-enabled environments. While the institution does not currently operate technical watermarking or provenance infrastructure, it promotes responsible disclosure, academic integrity, source attribution, and human verification practices when AI-generated content is used.

The institution encourages students and educators to identify AI-assisted work appropriately and to maintain accountability for the accuracy, originality, and integrity of submitted content. Fayston continues to monitor emerging standards and best practices related to AI-generated content transparency and provenance.

## Section 6 – Research & Investment to Advance AI Safety & Mitigate Societal Risks

### 28. Does your organization advance research and investment in the following areas?

- Safety
- Information integrity
- Explainability or interpretability
- System performance and outcomes (e.g. accuracy, consistency)
- Transparency
- Data quality and representativeness
- Robustness or reliability

**If yes, please describe key research or investment initiatives in the areas selected above (e.g., dedicated safety teams, funding of research programs, contributions to open-source safety tools, publishing research, partnerships and collaborative research initiatives). You may also indicate whether related outputs are publicly shared, shared with partners or within consortia or not publicly disclosed.**

Fayston advances responsible AI use through research, governance development, professional learning, and participation in international AI governance initiatives. The institution focuses on practical approaches to safety, transparency, information integrity, human oversight, explainability, reliability, and responsible deployment within educational settings.

Research and development activities include evaluation of AI-assisted decision-making, verification practices, accountability mechanisms, governance controls, educational impacts, and institutional risk management. These efforts inform institutional policies, professional development activities, governance reviews, and implementation guidance.

Fayston contributes to broader discussions through participation in international AI governance initiatives, accreditation activities, professional networks, presentations, publications, and collaborative projects. Outputs may be shared publicly, through professional communities, or through multi-stakeholder governance initiatives where appropriate.

Particular attention is given to preserving meaningful human judgment, supporting information integrity, promoting transparency, and ensuring that AI systems remain subject to appropriate human oversight in consequential educational contexts.

### 29. Does your organization pursue research or investment related to socio-economic or environmental considerations in the development and deployment of AI?

- Socio-economic considerations (e.g., AI adoption and productivity, workforce transitions, skills development, access to AI tools)

**If yes, please provide examples of relevant research or investment initiatives for the areas selected above.**

Examples:

- AI literacy
- workforce preparation
- student readiness
- responsible adoption
- access to AI tools
- future skills development

#### **Any further comments and implementation documentation.**

Fayston supports research, professional learning, and institutional implementation efforts related to the responsible use of artificial intelligence in education. Areas of focus include AI safety, transparency, information integrity, explainability, educational outcomes, and responsible governance.

The institution participates in national and international AI governance discussions and contributes to knowledge-sharing activities through professional networks, accreditation organizations, academic research, and international initiatives. Institutional activities emphasize human oversight, accountability, verification practices, and responsible decision-making when AI systems are used in educational settings.

Fayston also examines the socio-economic implications of AI adoption, including student preparedness, workforce readiness, digital literacy, equitable access to AI tools, and the development of future-ready competencies. These activities are intended to help students, educators, and institutional leaders navigate the opportunities and risks associated with rapidly evolving AI technologies.

As an educational institution deploying third-party AI systems rather than developing frontier AI models, Fayston's investments are primarily directed toward governance, policy development, professional learning, educational implementation, and institutional capacity building rather than technical AI model research.

## **Section 7 – Advancing Human and Global Interests**

**30. Does your organization support any digital literacy, education or training initiatives to improve user awareness and/or help people understand the nature, capabilities and limitations of advanced AI systems?**

Yes

**If yes, describe any digital literacy or training initiatives your organization supports (e.g., user education, public AI-education programs, school or university partnerships, community workshops). You may also indicate whether these efforts include or prioritise underserved or underrepresented communities.**

Fayston supports AI literacy and responsible AI education for students, educators, and school leaders. Activities include classroom instruction, faculty professional development, guidance on ethical AI use, academic integrity expectations, critical evaluation of AI-generated content, and discussions regarding the benefits, limitations, and risks of AI systems.

The institution emphasizes responsible use, human oversight, verification of AI-generated information, source attribution, transparency, and accountability. AI literacy efforts are integrated into educational practice and ongoing professional learning initiatives.

**31. Does your organization pursue AI projects that aim to deliver societal or public benefits, including through partnerships with civil society and community groups?**

Yes

**If yes, please provide examples, including any collaborations with civil society, community groups, or efforts to address broader societal challenges.**

Fayston seeks to advance the responsible and beneficial use of artificial intelligence through education, professional learning, institutional governance, and international collaboration. The institution promotes AI literacy among students, educators, and school leaders, helping stakeholders understand both the opportunities and limitations of AI systems.

AI-related educational activities emphasize critical thinking, responsible use, academic integrity, human oversight, transparency, accountability, privacy protection, and verification of AI-generated information. Students and educators are encouraged to use AI tools responsibly while maintaining independent judgment and personal accountability for decisions and submitted work.

Beyond the school community, Fayston contributes to broader public-interest discussions regarding AI governance and responsible deployment through participation in international initiatives, professional networks, accreditation communities, research activities, and knowledge-sharing efforts. These activities support the development of practical governance approaches that promote educational benefit while mitigating risks associated with AI adoption.

As an educational institution, Fayston's primary contribution is building human capacity, AI literacy, governance awareness, and responsible implementation practices that help prepare learners and educators to participate effectively in an AI-enabled society.

**Any further comments and implementation documentation.**

*No answer provided*