



GOVERNANCE FRAMEWORK

Child Safety and Wellbeing Framework

Policy, code of conduct, complaints procedure, public commitment, risk management plan and child-friendly summary

Organisation	Edexia Pty Ltd ABN 46 676 224 892
Version	1.0
Approved by	Priaav Salot, authorised delegate of the Chief Executive Officer
Accountable executive	Daniel Gibbon, Chief Executive Officer and interim Child Safety Lead
Effective date	14 October 2026
Review dates	First implementation review by 14 January 2027; annual review by 14 October 2027

Approval record Approved electronically by Priaav Salot on 14 October 2026 under delegated authority from Daniel Gibbon.

How to use this framework

This framework applies across Edexia's product, support, school visits, demonstrations, research, events and any other activity involving or affecting a person under 18. Each part is binding from the effective date. The action register records implementation work that strengthens the framework without delaying its adoption.

Contents

- Part 1 Child Safety and Wellbeing Policy
- Part 2 Worker Child Safe Code of Conduct
- Part 3 Child Safety Complaints and Concerns Procedure
- Part 4 Public Commitment to Child Safety and Wellbeing
- Part 5 Child and Youth Risk Management Plan
- Part 6 Child-friendly Safety Summary
- Appendix A Queensland Child Safe Standards mapping
- Appendix B Source framework and public references

Governance contacts

Child Safety Lead	Daniel Gibbon, Chief Executive Officer
Deputy contact	Priaav Salot, Executive Assistant to the Chief Executive Officer
Intake	admin@edexia.ai Subject: Child safety concern
Immediate danger	Call 000 before using Edexia's internal process

PART 1

Child Safety and Wellbeing Policy

Purpose

Edexia provides an online learning environment used by children and young people. This policy sets out how Edexia will prevent, identify and respond to harm involving children who interact with its products, people and services.

Edexia commits to the Universal Principle of cultural safety for Aboriginal and Torres Strait Islander children and the 10 Queensland Child Safe Standards.

Scope

This policy applies to every Edexia director, employee, contractor, consultant and volunteer. It applies to Edexia's online product, support channels, school visits, demonstrations, research, events and any other activity involving or affecting a person under 18.

Edexia is a technology provider and does not replace a school's supervision, duty of care, mandatory-reporting duties or safeguarding policies. That boundary does not reduce Edexia's own responsibility for its people, product, data, support and response to concerns involving the service.

Definitions

- **Child** means a person under 18.
- **Child abuse or harm** includes physical, sexual, emotional or psychological abuse, neglect, grooming, exploitation, discrimination and harm occurring through an online environment.
- **Child safety concern** means any disclosure, allegation, observation, complaint, incident, near miss or product behaviour that may indicate a child is unsafe or at risk.
- **Worker** means a director, employee, contractor, consultant or volunteer covered by this policy.
- **School** includes a school, education provider or other customer responsible for the learning activity and its users.
- **Child-impact assessment** means a documented assessment of how a proposed product, service, data or operational change may affect children's rights, safety, privacy and wellbeing.

Core commitments

Edexia will:

1. embed child safety and wellbeing in leadership, governance and culture;
2. inform children about their rights, listen to them and take their views seriously;
3. involve families, schools and communities in promoting child safety;
4. uphold equity, inclusion and cultural safety, including the Universal Principle;
5. ensure people working with children are suitable, supported and appropriately screened;
6. maintain child-focused processes for complaints and concerns;
7. train workers to recognise risks, respond to disclosures and meet their obligations;
8. design physical and online environments to promote safety and minimise harm;
9. review incidents, feedback, risks and controls to drive continuous improvement; and
10. keep accessible policies and procedures that explain how Edexia is safe for children.

Expected conduct

Everyone covered by this policy must:

- put a child's safety and wellbeing first;
- treat children fairly, respectfully and without discrimination;
- communicate in a professional, age-appropriate and observable way;
- use Edexia and school-approved channels for interactions involving students;
- avoid unnecessary one-to-one contact with a child and follow the school's supervision rules;
- never seek a child's personal contact details for a private or unrelated purpose;
- never engage in sexualised, coercive, degrading, intimidating or exploitative conduct;
- never create, request, store or share material that exploits, sexualises or harms children;
- act on concerns and disclosures promptly, without investigating beyond their role;
- preserve confidentiality while sharing information when required for safety or law; and
- report suspected breaches of this policy to the Child Safety Lead.

Responsibilities

Chief Executive Officer

The CEO is accountable for the child-safe governance system, resources, appointments, staff training and corrective actions. Child safety is a standing governance and operational risk item.

Child Safety Lead

The Child Safety Lead receives and triages concerns, coordinates immediate safety measures, maintains restricted records, assesses reporting obligations, supports affected children and families, and reports trends and actions to the CEO. A named backup must cover absences and any conflict involving the Lead.

Product and security leaders

Product and security leaders assess child-safety risks in feature design, access controls, content, AI behaviour, data handling, third-party services and incident response. Risks must be recorded in the Child and Youth Risk Management Plan before material releases. A child-impact assessment is required before a material change to a child-facing feature, adult-child interaction, data flow, AI behaviour, content-sharing capability or safety control.

All workers

All workers must read this policy, complete assigned training, follow screening requirements and immediately report any concern about a child's safety or wellbeing.

Voice, participation and accessibility

Edexia will provide age-appropriate ways for children to raise concerns and give feedback. Children will be taken seriously and may use a trusted adult, teacher, parent or carer to communicate with Edexia. Processes will consider disability, language, culture, family circumstances and other needs.

Edexia will seek feedback from schools, families and children when assessing child-safety controls. It will invite culturally safe input, including from Aboriginal and Torres Strait Islander stakeholders where relevant, without placing an unreasonable consultation burden on them.

Edexia will publish an age-appropriate summary of children's rights, teacher visibility, reporting options and what children can expect after raising a concern. That summary will be tested with children or an appropriate youth adviser before publication and after material changes.

Recruitment, screening and support

Before a role begins, Edexia will assess whether it involves direct or more than incidental contact with children and record the Blue Card or other screening requirement. A person must not perform a screened role until the required clearance is verified and linked to Edexia where required.

Role descriptions, onboarding and performance processes will state child-safety responsibilities. Workers will receive training appropriate to their role, including how to recognise and report harm, respond to a disclosure, protect privacy and use online environments safely.

Safe online and physical environments

Edexia will apply privacy, security and least-access controls to student information. Product and operational reviews will consider harmful content, inappropriate contact, misuse of AI, disclosure of personal information, impersonation, bullying, discrimination and risks affecting children with heightened vulnerability.

Edexia's current student-facing AI tutor uses compulsory prompt-level safeguards that prohibit full drafts, quotes and grading, treat student-authored context as untrusted data and direct wellbeing concerns to a trusted adult. Teachers can review student-AI conversations and add feedback. These controls reduce risk but do not guarantee that every AI response is safe or correct, and Edexia does not continuously monitor every conversation.

The product currently has no separate output-moderation pass for tutor responses. The standing notice that a teacher can read the AI conversation is also not equally prominent on desktop and mobile. These are open risks to be assessed and tracked in the Child and Youth Risk Management Plan, not capabilities to be implied by this policy.

Material product changes affecting children require layered safeguards appropriate to the risk, rather than reliance on a single prompt, policy or monitoring mechanism. Controls may include feature restrictions, age-appropriate design, access controls, event logging, reporting tools, human review, testing, school controls and proportionate account or feature restrictions.

School visits and demonstrations will follow the school's safeguarding and supervision requirements. Edexia workers must not arrange unsupervised student contact unless the activity has been approved, risk assessed and all required screening is complete.

Complaints, disclosures and incidents

Concerns are handled under the Child Safety Complaints and Concerns Procedure. Immediate danger must be addressed first, including contacting emergency services where necessary. Edexia will respond in a child-focused, timely, respectful and trauma-informed way, cooperate with relevant authorities and avoid any action that could compromise an external investigation.

No person will be disadvantaged for raising a genuine concern. Information will be restricted to people who need it to protect a child, investigate fairly or meet a legal obligation.

Records, review and continuous improvement

Child-safety records will be stored securely with restricted access and retained according to law and Edexia's approved retention requirements. The Child Safety Lead will review complaints, near misses, incidents and feedback for trends, without exposing children unnecessarily.

This policy and the Child and Youth Risk Management Plan will be reviewed at least annually, after a child-safety incident or complaint, after a material product or service change, and when relevant law or QFCC guidance changes.

Related documents

- Child Safety Complaints and Concerns Procedure
- Worker Child Safe Code of Conduct
- Public Commitment to Child Safety and Wellbeing
- Child-friendly Safety Summary
- Child and Youth Risk Management Plan
- Edexia Privacy Policy
- Edexia Security Measures
- Edexia Data Retention Policy

PART 2

Worker Child Safe Code of Conduct

Who this applies to

This Code applies to every Edexia director, employee, contractor, consultant and volunteer. It applies whenever a person's work involves or may affect a child, including through the product, support, research, demonstrations, school visits, events, data access and online communication.

Required conduct

Everyone covered by this Code must:

- put the safety, wellbeing, dignity and best interests of children first;
- treat children fairly, respectfully and without discrimination;
- listen to children and take concerns, disclosures and signs of harm seriously;
- use professional, age-appropriate and observable communication;
- use Edexia-approved or school-approved channels for child-related work;
- maintain appropriate boundaries and avoid unnecessary one-to-one contact;
- follow the host school's supervision, safeguarding and reporting requirements;
- protect student information and access it only for an authorised work purpose;
- consider disability, culture, language, age and other vulnerability factors;
- support the cultural safety of Aboriginal and Torres Strait Islander children;
- complete required child-safety training and screening before relevant work; and
- immediately report suspected harm, grooming, exploitation, unsafe conduct or a breach of this

Code.

Prohibited conduct

A person covered by this Code must not:

- engage in sexualised, exploitative, grooming, coercive, humiliating, threatening or abusive conduct involving a child;
- use private personal accounts, social media or personal contact details to communicate with a child for an Edexia purpose;
- arrange an unsupervised meeting with a child unless it has been specifically approved, risk assessed and all required screening is complete;
- seek or maintain a secret relationship, offer inappropriate gifts or favour one child in a way that creates dependency or obligation;
- photograph, record or publish identifiable material involving a child without documented authority and a legitimate purpose;
- copy, download, disclose or retain student information beyond the authorised work purpose;
- upload identifiable student information or work to an unapproved consumer AI tool;
- use Edexia access to monitor a child for a personal purpose;
- ignore, suppress or retaliate against a complaint or safety concern;
- promise a child absolute secrecy about a safety disclosure; or
- conduct an informal investigation that could expose a child to further harm or compromise an external investigation.

Product, AI and support conduct

Workers must not bypass product safeguards, enable prohibited functionality or make unsupported claims about what the product prevents. A worker reviewing student content or conversations must do so only for an authorised support, safety, security or quality purpose and must minimise exposure to identifiable information.

If a worker sees distress, suspected abuse, grooming, sexual exploitation, harmful content or a credible threat through the product or support channels, they must preserve relevant evidence, restrict unnecessary access and escalate immediately under the Child Safety Complaints and Concerns Procedure.

Edexia's AI safeguards assist prevention but do not replace human oversight, the school's duty of care or the obligation to report concerns.

School visits and live activities

Before any activity involving children, the activity owner must identify the supervising school contact, confirm relevant host requirements, assess the contact level and screening requirements, and record any heightened risks. Edexia personnel must remain within the approved activity and must not remove a child from the school's supervision.

Reporting and consequences

Concerns and breaches must be reported to the Child Safety Lead or, if that person is unavailable or conflicted, to the CEO or nominated backup. Immediate danger must be addressed first, including by contacting emergency services where necessary.

A breach may result in removal from child-related duties, access restriction, investigation, disciplinary action, termination of engagement, notification to the school or authorities, or other proportionate action. Reporting a concern in good faith is protected from retaliation.

Acknowledgement

Before child-related work, each person must confirm that they have read, understood and will follow this Code, the Child Safety and Wellbeing Policy and the Child Safety Complaints and Concerns Procedure.

PART 3

Child Safety Complaints and Concerns Procedure

Purpose and scope

This procedure covers complaints, concerns, disclosures and allegations involving the safety or wellbeing of a child or vulnerable young person in connection with Edexia's people, products, services or online environment. It applies whether the concern is raised by a child, family member, teacher, school, worker, contractor or third party.

Where a concern involves a school-managed account or activity, Edexia will coordinate with the school's nominated safeguarding contact where appropriate. Edexia will not assume that notifying the school discharges any separate duty to notify police, child protection, QFCC or another authority.

It is separate from the Privacy Policy's privacy-complaints process, although a matter may require both procedures.

How to raise a concern

A person may:

- email admin@edexia.ai with the subject "Child safety concern";
- tell an Edexia worker, who must pass the concern to the Child Safety Lead immediately; or
- ask a trusted adult, school safeguarding contact, parent or carer to report on their behalf.

Edexia will acknowledge a report promptly, explain the next safe step in age-appropriate language and provide an accessible alternative where email is unsuitable.

If a child is in immediate danger, contact emergency services on 000 before using Edexia's process. Edexia will provide a more accessible communication method where needed.

First response

The person receiving the concern must:

1. listen calmly and take the person seriously;
2. prioritise immediate safety and urgent medical or protective needs;
3. not promise secrecy, blame the child or ask leading or investigative questions;
4. record the person's own words and the time, date and circumstances;
5. preserve relevant evidence without circulating it unnecessarily; and
6. escalate the matter immediately to the Child Safety Lead or, if conflicted, the CEO or nominated backup.

Triage and external reporting

The Child Safety Lead must promptly assess:

- whether a child faces immediate or ongoing risk;
- what support and protective measures are required;
- whether police, child protection, QFCC, a school, insurer or another regulator must be notified;
- whether the matter may fall within a reportable conduct scheme or another mandatory-reporting obligation;
- whether a worker should be removed from child-related duties while the matter is assessed; and
- what information may lawfully be shared to protect the child.

Edexia will obtain legal advice where the reporting duty or investigative boundary is unclear. It will cooperate with relevant authorities and will not conduct an internal process that could prejudice a police, child-protection or regulatory investigation.

Child-focused handling

Edexia will:

- explain the process in language the child can understand;
- ask what support, communication method and trusted person the child wants where appropriate;
- respect cultural identity, disability, family circumstances and other needs;
- provide culturally safe support for Aboriginal and Torres Strait Islander children;
- minimise repeated retelling and exposure to potentially traumatic material;
- protect privacy while making necessary safety disclosures;
- keep the complainant reasonably informed of progress and outcome; and
- prohibit retaliation against a person who raises a genuine concern.

Fair assessment and outcome

The Child Safety Lead will create a restricted case record, identify the applicable policy and law, coordinate any permitted fact-finding, and give affected people procedural fairness where this does not compromise a child's safety or an external investigation.

Outcomes may include immediate safeguards, product or access changes, worker directions, training, disciplinary action, referral to authorities, support for the child and family, policy changes, or a finding that the concern could not be substantiated. A lack of substantiation does not prevent Edexia from improving controls where a risk was identified.

Records and continuous improvement

Case records must be accurate, dated, access-restricted and stored separately from routine support material. Retention and disclosure will follow applicable law and Edexia's approved retention and security requirements.

At least quarterly during the first year after adoption, the Child Safety Lead will provide the CEO with de-identified trends, timeliness, control failures and corrective actions. This procedure must be reviewed after any material complaint or incident and at least annually.

PART 4

Public Commitment to Child Safety and Wellbeing

Our commitment

Edexia is committed to the safety, wellbeing and dignity of every child and young person who uses our products or interacts with our people.

We put children's safety at the centre of our decisions. We do not tolerate child abuse, harm, exploitation, discrimination or conduct that puts a child at risk. We listen to children and take their views and concerns seriously. We aim to make our online environment safe, inclusive and accessible, and to uphold the cultural safety of Aboriginal and Torres Strait Islander children.

Where students use Edexia's AI tutor, their teacher can review the conversation and add feedback. Edexia does not continuously monitor every conversation, and AI can make mistakes, so we provide clear reporting routes and use layered product, people and process controls rather than relying on one safeguard.

Everyone who works for or with Edexia shares responsibility for preventing harm, following our child-safety requirements and reporting concerns. We respond to concerns promptly, respectfully and in a child-focused way, and we cooperate with schools, families and relevant authorities.

Children, families, schools and community members may raise a child-safety concern through a trusted adult or by contacting admin@edexia.ai with the subject "Child safety concern". If a child is in immediate danger, contact emergency services on 000.

We review our policies, product controls, feedback and incidents so that we continue to improve how we protect children and support their wellbeing.

PART 5

Child and Youth Risk Management Plan

Purpose

This plan identifies foreseeable risks of harm to children arising from Edexia's online learning environment, support, demonstrations, school visits and third-party services. It sets controls, owners and review triggers. It must be used with the Child Safety and Wellbeing Policy and the Child Safety Complaints and Concerns Procedure.

Risk method

For each risk, the owner assesses likelihood and consequence, records existing controls, assigns further actions and a due date, and documents residual risk. A control is not treated as implemented until evidence exists that it operates in practice.

Risks involving children with heightened vulnerability require specific consideration, including disability, age, language, cultural identity, family circumstances and Aboriginal and Torres Strait Islander cultural safety.

Initial risk register

Risk	Minimum controls and actions	Owner	Evidence required before closure
Inappropriate adult-child contact	Use school-approved and observable channels; prohibit private or unrelated contact; avoid unsupervised contact; assess and record Blue Card requirements by role	Child Safety Lead	Role assessments, contact protocol, screening register
Unsafe or incorrect AI tutor response	Existing prompt safeguards prohibit full drafts, quotes and grading, fence student text as untrusted and contain wellbeing escalation; add child-safety test cases, incident route and an evidence-based decision on output moderation	Product lead and Child Safety Lead	Current adversarial test results, approved residual-risk decision, incident playbook
Harmful, sexualised, discriminatory or age-inappropriate content	Clear prohibited-content rules; reporting path; layered prevention and detection proportionate to available content types; preservation and escalation process	Product lead	Review record, test cases, incident playbook
Bullying, harassment or coercion through the service	Clear conduct rules; accessible reporting; rapid protective action; school escalation route	Product lead and Child Safety Lead	Published rules, tested report flow, response log
Excessive or inappropriate collection, access or disclosure of student information	Data minimisation, role-based access, encryption, logging, incident response and school-authorized access	Security lead	Current Security Measures, access review, incident test
Impersonation or unauthorised account access	Authentication controls, role verification, least privilege, monitoring and revocation process	Security lead	Control test and access-review record

Risk	Minimum controls and actions	Owner	Evidence required before closure
Student does not understand who can see an AI conversation	Publish the child-friendly summary; add an equally prominent teacher-visibility notice on desktop and mobile; test comprehension with students	Product lead	UI evidence at supported breakpoints and comprehension notes
Unsafe school visit, demo, research or event	Follow host-school safeguards; named supervising adult; no unsupervised student contact; pre-activity risk check	Activity owner	Activity checklist and host approval
Worker or contractor is unsuitable for child-related duties	Role-based screening assessment, reference and identity checks, required Blue Card verification, conduct agreement and training	CEO and Child Safety Lead	Screening register and onboarding record
Concern or disclosure is missed, mishandled or re-traumatises a child	Child-focused complaints procedure; monitored intake; trained responders; external-reporting assessment; restricted records	Child Safety Lead	Intake test, training record, case audit
Third-party service creates child-safety or data risk	Supplier due diligence, contractual safeguards, least-data use, access controls, incident notification and periodic review	Security lead	Supplier register, assessment and contract record
Cultural safety or accessibility needs are overlooked	Accessibility review; inclusive design; culturally safe feedback; specific consultation where relevant	Product lead and Child Safety Lead	Review notes, actions and feedback evidence
Control degrades after product or organisational change	Child-safety review in release and vendor processes; annual policy review; post-incident and post-change review	CEO and relevant owner	Review calendar, release/vendor checks, action log
Child-facing feature launches without considering the child's best interests	Require a documented child-impact and privacy-impact assessment before material child-facing changes	Product lead and Privacy Officer	Completed assessment linked to release decision

Review triggers

The plan must be reviewed:

- at least annually and quarterly during the first year;
- before a material product feature, data flow or child-facing service launches;
- before a new activity involving direct or more than incidental contact with children;
- after a complaint, incident, near miss, external finding or material control failure;
- after relevant legal or QFCC guidance changes; and
- when feedback from children, families, schools, workers or communities identifies a new risk.

Each review must record participants, evidence considered, changes, unresolved risks, owners and due dates. The CEO accepts any residual high risk in writing.

Implementation action register

The policy suite, code, complaints procedure and risk plan took effect on 14 October 2026. The following actions operationalise and strengthen the framework. An item is closed only when the owner records evidence that the control operates in practice.

Action	Owner	Due	Status at adoption
Adopt this framework and appoint accountable roles	CEO and authorised delegate	14 Oct 2026	Complete
Confirm and test admin@edexia.ai as the child-safety intake route	Child Safety Lead	15 Oct 2026	Approved route; test pending
Publish the public commitment and framework on edexia.com	CEO and website owner	16 Oct 2026	Ready for publication
Brief workers and record policy and Code acknowledgements	Child Safety Lead	31 Oct 2026	Scheduled
Assess Blue Card and other screening requirements by role and activity	Child Safety Lead	31 Oct 2026	Open
Complete the first online-product child-safety risk review	Product and security leads	30 Nov 2026	Open
Decide and record the control response to the absence of an AI-output moderation pass	Product lead and Child Safety Lead	30 Nov 2026	Open
Make teacher-visibility notices equally prominent on desktop and mobile	Product lead	30 Nov 2026	Open
Add a child-impact assessment gate to material child-facing releases	Product lead	30 Nov 2026	Open
Test the complaint and incident escalation pathway	Child Safety Lead	31 Oct 2026	Open
Test the child-friendly summary with students or an appropriate youth adviser	Child Safety Lead	14 Jan 2027	Open
Record the first governance review and residual risks	CEO	14 Jan 2027	Open

PART 6

Your safety when using Edexia

What you can expect

- You should be treated fairly and respectfully.
- You can say when something feels wrong, unsafe or confusing.
- You can ask a teacher, parent, carer or another trusted adult for help.
- Your teacher can read your conversation with Edexia's AI and may add feedback.
- Edexia staff do not continuously read every conversation. Authorised people may review information

when needed for support, safety, security or legal reasons.

- The AI can make mistakes. If its response worries you or seems wrong, stop and tell your teacher or another trusted adult.
- No Edexia worker should ask you to keep a relationship or conversation secret, contact them through a personal account, or meet them alone outside an approved school activity.

If something happens

If you feel unsafe or think another child may be unsafe:

1. move away from immediate danger if you can;
2. tell a teacher, parent, carer or another trusted adult;
3. ask them to contact Edexia at admin@edexia.ai with the subject "Child safety concern"; and
4. if someone is in immediate danger, call 000.

You will not be in trouble for raising a genuine concern. Edexia will take you seriously, share the information only with people who need it to help, and try to avoid making you repeat the story more than necessary.

Help us improve

Children and young people should help shape how online learning is kept safe. You can give feedback through your teacher or a trusted adult. Edexia will test whether students can understand this summary and improve it using their feedback.

Appendix A

Queensland Child Safe Standards mapping

This mapping shows where the framework addresses the Universal Principle and the 10 Queensland Child Safe Standards. Operational evidence must be maintained separately and reviewed through the risk plan.

Requirement	Framework coverage
Universal Principle	Policy sections 4, 7 and 9; Code sections 2 and 5; complaints procedure section 5; risk plan sections 2 and 3
1 Leadership, governance and culture	Policy sections 4, 6 and 11; approval record; risk plan sections 4 and 5
2 Children are safe, informed and participate	Policy section 7; public commitment; child-friendly summary
3 Families and communities are informed and involved	Policy section 7; complaints procedure sections 2 and 5; public commitment
4 Equity is upheld and diverse needs respected	Policy sections 4, 7 and 9; Code section 2; complaints procedure section 5
5 Suitable people are supported	Policy sections 6 and 8; Code sections 2 and 7; risk plan screening controls
6 Child-focused complaints processes	Policy section 10; Child Safety Complaints and Concerns Procedure
7 Knowledge, skills and awareness	Policy sections 6 and 8; Code section 7; implementation action register
8 Safe physical and online environments	Policy section 9; Code sections 4 and 5; risk plan section 3
9 Review and continuous improvement	Policy section 11; complaints procedure section 7; risk plan section 5
10 Policies and procedures document child safety	The complete framework and associated approval, publication and acknowledgement records

Appendix B

Source framework and public references

Edexia developed this framework against the Queensland child-safe framework and reviewed comparable Australian education and online-safety policies. The legislation and QFCC guidance control where a peer document differs.

- **Queensland Family and Child Commission:** [Child Safe Standards resources](#)
- **Queensland legislation:** [Child Safe Organisations Act 2024](#)
- **eSafety Commissioner:** [Safety by Design and child online-safety resources](#)
- **Academyship:** [Child safety policy](#)
- **3P Learning:** [Privacy policy and children's privacy approach](#)
- **EEVA:** [Child safe policy](#)
- **The 3rd House:** [Child safety and wellbeing policy](#)

Document control

Version	Date	Change
1.0	14 October 2026	Initial adoption
Next review	14 January 2027	First implementation review