BRIDGELEA PRIMARY SCHOOL

Bridgelea Primary School	Bridgelea Primary School
Bridgelea Road	Plymouth Grove West
Withington	Longsight
Manchester	Manchester
M20 3FB	M13 0AQ

POLICY INFORMATION

Policy Title	Artificial Intelligence
Lead Officer	Kelly Eyre
Status	Non-Statutory
Implemented By	Senior Leadership Team
Presented By	Kelly Eyre
Ratified By	Full Management Group
Approval Date	October 2026
Last Reviewed	New Policy
Review Date	Autumn 2027

UNDERSTANDING PEOPLE

Communication • Inclusion • Safety • Aspiration

Our Vision

Our vision of **Understanding People** captures our core purpose.

At Bridgelea, we support children, families and communities to develop a deeper understanding of themselves and others. Through nurturing relationships, high-quality teaching and an ambitious curriculum, we help every child develop the knowledge, skills and confidence they need to thrive now and in the future.

We believe that understanding behaviour, emotions, learning and relationships creates the foundation for success, wellbeing and positive life outcomes.

THE BRIDGELEA VALUES

Communication

We believe every child deserves to be heard and understood.

We help children develop their speech, language and communication skills so they can express themselves, build relationships and access learning successfully. Staff use visual supports, clear language and personalised strategies to make communication accessible for everyone.

Inclusion and Partnership

We know that children achieve best when school and home work together.

We build strong partnerships with families and work closely with external agencies, including health, social care and mental health services, to ensure children receive the support they need. We celebrate difference and ensure every child feels welcomed, respected and included.

Safety and Wellbeing

Children learn best when they feel safe, secure and cared for.

Safeguarding and wellbeing are at the heart of everything we do. We help children develop strategies to manage emotions, build resilience and make safe choices both in school and beyond. Our nurturing environment supports the wellbeing of children, families and staff alike.

Aspiration and Independence

We want every child to believe in themselves and their future.

We encourage children to develop confidence, independence and the skills they need for life. Through high expectations, meaningful experiences and positive relationships, we help children become resilient learners who are ready for their next steps.

THE BRIDGELEA WAY

At Bridgelea we:

- Place nurture and relationships at the heart of our practice.
- Prioritise communication and language development.
- Provide an ambitious and personalised curriculum.
- Teach children about rights, responsibilities and respect.
- Develop independence, resilience and preparation for adulthood.
- Work in partnership with families and external agencies to secure the best possible outcomes for every child.

Our curriculum is designed around the needs of our children. It is flexible, ambitious and nurturing, supporting progress both academically and personally whilst preparing children for success in school, their community and later life.

RIGHTS RESPECTING SCHOOL

As a UNICEF Rights Respecting School, children's rights underpin our policies, curriculum and daily practice.

Through their work with the School Council, children identified ten key articles from the United Nations Convention on the Rights of the Child (UNCRC) that they believe are particularly important to life at Bridgelea. These articles help guide our work whilst recognising that all rights are universal, indivisible and equally important.

Bridgelea Key Articles

Article 12

Children have the right to give their opinions and for adults to listen and take them seriously.

Article 13

Children have the right to seek, receive and share information and ideas.

Article 15

Children have the right to choose friends and join groups.

Article 24

Children have the right to the best possible healthcare, clean water, healthy food and a safe environment.

Article 27

Children have the right to a standard of living that meets their needs.

Article 28

Children have the right to a good quality education.

Article 29

Education should help children develop their talents and abilities, respect others and care for the environment.

Article 30

Children have the right to enjoy their own culture, language and religion.

Article 31

Children have the right to rest, relax and play.

Article 39

Children have the right to support and recovery if they have experienced harm, neglect or abuse.

OUR NURTURING APPROACH

Bridgelea's practice is underpinned by the principles of nurture.

The nurturing approach provides opportunities for children and young people to experience and develop the social, emotional and relational skills that may have been disrupted through adverse experiences. Through nurturing relationships, children develop resilience, confidence, self-regulation and the ability to engage successfully in learning and life.

The Six Principles of Nurture

1. Children's learning is understood developmentally.
2. The classroom offers a safe base.
3. The importance of nurture for the development of wellbeing.
4. Language is a vital means of communication.
5. All behaviour is communication.
6. The importance of transitions in children's lives.

EQUALITY AND INCLUSION STATEMENT

Bridgelea Primary School is committed to providing an inclusive environment where all pupils, staff, families and visitors are treated with dignity, respect and fairness. We actively promote equality of opportunity, challenge discrimination and celebrate diversity within our school community.

SAFEGUARDING STATEMENT

Safeguarding is everyone's responsibility.

Bridgelea Primary School is committed to safeguarding and promoting the welfare of children and young people. All policies should be read alongside the school's Child Protection and Safeguarding Policy, Behaviour Policy, Staff Code of Conduct, Whistleblowing Policy and the most recent version of *Keeping Children Safe in Education (KCSIE)*.

APPLYING THIS POLICY

This policy should be read in the context of Bridgelea's vision, values, nurturing approach and commitment to children's rights. The implementation of this policy is intended to support children to be safe, understood, successful and prepared for their next stage of learning and life.

---

1 Purpose and scope

Bridgelea will use artificial intelligence (AI) to support teaching, communication, accessibility and staff efficiency while protecting children's safety, rights and personal information. This policy sets the conditions for selecting tools, using information, reviewing outputs and responding to concerns. Human relationships and professional judgement remain central to our work as a specialist Pupil Referral Unit (PRU).

This policy applies to staff, governors or management committee members, volunteers, trainees, contractors and pupils using AI in connection with school business. It covers school and personal devices, remote working, and AI features embedded in existing software, including assistants, transcription, image generation and tools connected to school files.

Rights respecting approach

Bridgelea's nurturing, trauma-informed approach and commitment as a UNICEF Rights Respecting School guide decisions about AI. We consider children's best interests, listen to their views in accessible ways, and assess whether a proposed use supports learning and inclusion without exposing children to avoidable harm.

Relevant UN Convention on the Rights of the Child articles include non-discrimination (2), best interests (3), participation (12), expression and information (13 and 17), privacy (16), protection from harm (19), support for children with disabilities (23), education and development (28 and 29), and protection from exploitation (36). These are the school's applications of the rights, not quotations from the Convention.

Key terms

AI refers to systems that perform tasks such as generating content, recognising patterns or making predictions. Generative AI produces text, images, audio, video or other content. Its outputs may be inaccurate, biased or fabricated. A Data Protection Impact Assessment (DPIA) identifies and reduces risks to people from a proposed use of personal data.

2 Responsibilities

Headteacher and AI Lead

The Headteacher owns this policy and the live Approved AI Tools Register. They approve specific tools and uses in writing after the necessary advice and checks; arrange training; ensure conditions are implemented; and suspend use where safety or compliance is uncertain. They report implementation, incidents, benefits and unresolved risks to the management group at least annually.

Management group or management committee

The school's formally constituted management group approves this policy, challenges the adequacy of safeguards and resources, and reviews the Headteacher's reports. References to the management group throughout this policy include the management committee where that is the school's governance arrangement.

Designated Safeguarding Lead

The Designated Safeguarding Lead (DSL) assesses safeguarding implications, advises on pupil-facing tools and vulnerable pupils' needs, coordinates safeguarding responses and ensures relevant risks are covered in staff updates and safeguarding procedures.

Data Protection Officer

The Data Protection Officer (DPO) advises on lawful processing, supplier arrangements, privacy information, DPIAs, individual rights and data breaches. The school remains responsible for its

decisions; DPO advice must be documented. The existing policy identifies Global Policing as the DPO service; the current service and contact route must be confirmed before adoption.

Technical support provider

Technical support advises on security, account management, access to school information, filtering and monitoring, and safe deployment. It implements agreed settings and helps contain incidents. The existing policy identifies One Education as the provider; the current service and contact route must be confirmed before adoption.

Staff and other authorised adults

- Use only tools, accounts, features, purposes and data types authorised in the live register. Complete required training before use.
- Check outputs against reliable sources and the needs of the intended audience. Remain accountable for decisions and work produced.
- Report concerns and accidental disclosures immediately. Seek advice before proceeding if permission or data status is unclear.
- Do not activate new AI features, integrations or recording assistants for school business without approval. Contractors must meet the same relevant safeguards through their contracts.

3 Approval of tools and uses

Approval applies to a specified product, account type, configuration, users, purpose and data category. A brand name, paid subscription or existing school software licence does not give blanket approval. Trials must be assessed and authorised before use with school information or pupils.

Checks before approval

- Identify the educational or operational benefit, alternatives and how benefit will be evaluated. Consider accessibility, equality, children's rights and workload.
- Record the intended users, pupil ages, supervision, permitted features and provider age and account restrictions. Obtain DSL advice for pupil-facing or safeguarding-related uses.
- Check supplier terms, privacy information, security, model-training practices, human access to content, retention and deletion, subprocessors and any overseas processing. Obtain DPO advice where personal data is involved.
- Assess the specific workflow, including access to emails, files, connected services, prompts, attachments, audio, images and generated outputs. Record a DPIA screening decision; complete a DPIA before processing where required.
- Check account controls, least-privilege access, multi-factor authentication where available, filtering and monitoring, reporting routes and whether integrations or features need to be disabled.
- Test suitability using fictional or genuinely anonymous material. Record limitations, review arrangements, staff training and how access can be suspended.

The Headteacher records the decision and conditions in the live register, supported by DPO, DSL and technical advice as appropriate. No approval may override the prohibitions in section 7 or unresolved legal requirements. Where a DPIA identifies high residual risk, processing must not begin until the required consultation with the ICO has been completed.

Maintaining approval

Review each approval at least annually and before material changes to features, models, users, purposes, data, contracts or integrations. Review after relevant incidents or guidance changes. Pause affected uses if safeguards cannot be maintained. General policy approval does not automatically approve every tool listed in Appendix A.

Microsoft 365 Copilot

Where its exact school-managed service and intended use are approved, Microsoft 365 Copilot is the preferred platform for school business. The register must identify the service, licence and account arrangements, permitted connected data and enabled features. Consumer accounts and other Copilot services are not covered automatically. Access to school files must be checked before enabling connected features.

4 Personal data and confidential information

The default is to use fictional examples, public information or genuinely anonymised material. Staff must not put personal data or confidential school information into an AI tool unless the exact processing activity and data categories have been expressly authorised under this section and entered in the live register.

This restriction covers pupil and staff information; child protection and CPOMS records; education, health and care plans (EHCPs); medical, attendance and behaviour information; personnel records; and information from social care, police or other agencies. It also covers photos, voices, recordings, document metadata, linked files and information the tool retrieves automatically.

Conditions for exceptional use

Before authorising personal-data processing, the school must document why it is necessary and proportionate, whether a less intrusive method would meet the need, the lawful basis and any additional conditions for special category or criminal offence data. DPO advice, appropriate supplier terms and international-transfer safeguards must be recorded where relevant. Approval must specify access controls, data minimisation, retention, deletion and the information provided to affected people.

A DPIA screening decision is required for each proposed personal-data use. Complete a DPIA before any use likely to create high risks to people's rights and freedoms. As a school safeguard, a DPIA is also required before AI processing of identifiable safeguarding records, EHCPs, medical or behaviour records. A DPIA or Headteacher approval does not, by itself, make processing lawful.

Anonymisation

Removing a name is not enough if a person can still be identified from context or other information reasonably available. Replacing a name with "Pupil A" is pseudonymisation where the person remains identifiable, and must be handled as personal data. In a small PRU, age, diagnosis, a distinctive incident and family circumstances may identify a child.

Use general learning needs or fictional scenarios instead of detailed case histories. Do not upload identifiable information to an unapproved service in order to anonymise it. If uncertain, consult the DPO before use.

Storage and access

Use approved school accounts and storage. Do not allow school data or pupils' work to be used for general model training without separate documented authorisation addressing data protection and copyright. Apply the school's retention schedule to necessary records; avoid keeping prompts or outputs containing personal information without a defined purpose. The school must ensure, with DPO advice, that relevant processing records and privacy notices are updated, and that access, correction and other applicable rights can be addressed.

5 Permitted staff uses and output checks

Within their recorded approval, staff may use AI to draft lesson plans, questions, model examples, presentations, policies, agendas, newsletters and general correspondence; adapt reading materials; create visual supports; and assist with research or analysis. Approval for one purpose does not extend to another. All uses remain subject to section 4.

Teaching and inclusion

Staff must adapt materials to the curriculum and individual pupils' needs, including special educational needs and disabilities (SEND) and social, emotional and mental health (SEMH) needs. Use general descriptions or fictional examples unless a specific personal-data use is approved. Check that materials support learning rather than remove opportunities to practise, reason and communicate.

AI may assist with question generation, assessment preparation and feedback drafting. Qualified staff make final assessment judgements and evaluate pupil progress. AI must not diagnose SEND or mental health conditions, prescribe interventions or replace specialist assessment.

Checks before use or sharing

- Verify facts, calculations, references and quotations against reliable sources. Check current official sources for legal, safeguarding and policy statements.
- Review for bias, stereotypes, harmful content, accessibility, cultural context and age suitability. Ensure images and examples respect children's dignity.
- Check confidentiality, copyright, licences and permissions for source material and outputs. Do not present invented evidence, quotations or experiences as genuine.
- Check that translations communicate the intended meaning. Important safeguarding, consent, medical or other consequential communications require a competent human language check or appropriate interpreting support.
- Read and approve the complete final output before it is issued, published, recorded or used with pupils. No automatic sending, publishing or modification of school records is permitted without separately approved controls.

Transparency and records

The responsible author must acknowledge material AI assistance in substantive policies, reports, research and decision-support documents, for example in a drafting note naming the tool, purpose and human reviewer. Routine spelling or grammar assistance does not require a public label. AI-generated media must be labelled where people could otherwise mistake it for a genuine image, recording or event.

Pupils should use a simple age-appropriate acknowledgement when AI assistance is permitted. An acknowledgement does not authorise otherwise prohibited use. Staff must retain necessary evidence of sources, checking and approval in the normal school record, without creating unnecessary copies of sensitive prompts.

6 Pupil access and participation

Pupils may interact only with a specifically approved pupil-facing feature for an agreed educational activity under appropriate staff supervision. Staff approval for a product does not permit pupil use. Provider age restrictions and account terms must be checked and followed; parental permission does not override them.

A teacher demonstration using an approved adult account is different from a pupil interacting with the service. Staff must check that demonstrations are permitted, review material before display where practicable, and avoid exposing pupils to unfiltered live content. Pupils must not use staff credentials.

- Record permitted ages or groups, school-managed account arrangements, session limits and supervision in the register. Test filtering, monitoring and content controls with technical support.
- Teach pupils not to share names, photographs, voices, contact details or private experiences with a chatbot unless a specific supervised activity and data use have been authorised.
- Explain that AI can sound convincing while being wrong and does not have human understanding or relationships. Teach pupils to check information and tell a trusted adult about troubling content.
- Assess each pupil's communication, safeguarding and emotional needs. Provide accessible explanations and an appropriate alternative where the activity is unsuitable.
- Set clear expectations about permitted assistance and acknowledgement. Do not use an AI-detection score as the sole evidence of misconduct.

Pupil and parent feedback will inform evaluation. Pupils will learn about AI, misinformation, privacy and responsible creation in ways suited to their development. No pupil should be disadvantaged by lack of a paid service or personal account at home.

7 Prohibited uses and human decisions

AI must not determine safeguarding thresholds, assign child-risk scores, recommend whether a safeguarding referral should be made, or make decisions on exclusions, sanctions, admission, placement, recruitment or staff performance. Authorised staff must assess evidence and make accountable decisions. AI may support an expressly approved administrative task, but must not substitute for that assessment.

General-purpose chatbots must not be used as counsellors, emotional companions or substitutes for trusted adults. Staff must not use AI to impersonate people deceptively, create exploitative or abusive content, manipulate pupils, circumvent controls, or fabricate school records. Creating sexualised images of children, including synthetic images, is prohibited. Approval under this policy cannot authorise these activities.

8 Safeguarding and incident response

AI-related concerns are managed through the school's established safeguarding, data-breach and security procedures. Risks include deepfakes, nudification, bullying, grooming, exploitation, impersonation, fraud and harmful or misleading content. Staff must act promptly and must not wait for an AI response or for certainty before raising a concern.

Immediate staff actions

- Stop the affected activity and support the pupil or other person involved. Follow emergency procedures if someone is in immediate danger.
- Report safeguarding concerns immediately to the DSL or deputy. If neither is available, follow the safeguarding policy's escalation route without delaying necessary action. Follow the separate procedure for allegations about staff or the Headteacher.
- Report accidental uploads, unexpected disclosure, unauthorised access or unsafe integrations immediately to the Headteacher or nominated breach lead, DPO and technical support through established incident routes. Where safeguarding is also involved, notify the DSL as well.
- Record the time, tool, account, nature of the issue, information involved and action already taken. Preserve appropriate evidence securely under DSL, DPO or technical direction. Do not circulate harmful material, investigate suspected child sexual abuse imagery yourself, or copy it into CPOMS.
- Do not assume deleting a conversation removes supplier copies. Do not conceal an incident or delay reporting while attempting to fix it.

School response and follow up

The DSL coordinates the safeguarding response, records relevant concerns on CPOMS in accordance with safeguarding procedures, and arranges appropriate referrals and support. DPO and technical support advice informs containment, access suspension, supplier contact and secure deletion requests.

The school assesses personal-data breaches promptly and records the assessment, decisions and actions. It follows applicable reporting deadlines, including notifying the ICO without undue delay and within 72 hours of awareness where required, and notifying affected individuals without undue delay where the legal high-risk threshold is met. Staff must report internally immediately so that this assessment can take place.

The Headteacher records lessons learned, revises controls and decides whether use may resume after relevant advice. Staff and pupils receive any necessary support or updated guidance. Complaints follow the school's Complaints Policy; privacy rights and concerns are referred to the DPO.

Contact routes

Before adoption, insert or link the current staff-accessible contact details for the DSL and deputy, Headteacher or breach lead, DPO and technical support, including urgent and out-of-hours arrangements. These contacts must also be available through the existing safeguarding and breach procedures.

9 Parents and carers

Bridgelea will explain significant pupil-facing AI uses in accessible language, including their purpose, supervision, information handling and how to raise concerns. Relevant privacy notices must explain personal-data processing before it begins. Where consent or permission is required, the school will obtain it through an appropriate process; consent is not the default lawful basis for every school activity.

The school will offer proportionate guidance through newsletters, website resources, discussions and workshops where useful. It will listen to concerns, consider reasonable adjustments and offer suitable alternatives where needed. Families will not be expected to purchase AI products for compulsory learning.

10 Training and implementation

Staff must receive training before using approved AI tools and when a material change affects their use. Induction and refresher training will cover tool restrictions, anonymisation, output checking, safeguarding risks, copyright, bias, privacy and incident reporting. The AI Lead will maintain a record of training and provide role-specific support. Governors will receive sufficient information to challenge and oversee implementation.

Before this revision takes effect, the Headteacher will confirm the approving body and contact routes; reconcile existing tools with Appendix A; complete or check required assessments; communicate the live register to staff; and arrange the necessary training. Unconfirmed tools or uses must not be treated as approved under this revision.

11 Related policies

Read this policy alongside the Child Protection and Safeguarding Policy, Online Safety Policy, Data Protection Policy and breach procedure, ICT Acceptable Use Policy, Staff Code of Conduct, SEND Policy, Equality Policy, Complaints Policy, Positive Relationships and Communication Policy, relevant behaviour procedures and the Bridgelea Playbook. Confirm the current local titles before adoption. Statutory duties and safeguarding procedures continue to apply.

12 Monitoring and review

The AI Lead will monitor compliance, educational benefit, workload effects, accessibility, bias, incidents and feedback from pupils, families and staff. Review the live register at least annually and when material changes occur. Report findings and unresolved risks to the management group annually, escalating serious matters promptly.

Review this policy within 12 months of adoption and earlier following relevant legislative or guidance changes, significant developments in technology, serious incidents or evidence that safeguards are ineffective. Record the approving body, effective date, version and next review date after adoption.

Appendix A Tools requiring confirmation

The products below were listed in the previous policy. This table preserves that list for reconciliation; it does not certify the licences, settings, assessments or approval evidence. Each tool must have a completed approval record under Appendix B before being shown as active in the live register. Until then, its status under this revision is pending confirmation.

Tool named in previous policy	Intended users and purposes	Details to confirm
Microsoft 365 Copilot	Staff; drafting, presentations, communications and approved analysis.	Exact service, licence, school account, connected data, enabled features and permitted data categories.
KeyGPT	Staff and governors; policy drafting, leadership and research.	Product/account terms, permitted inputs, retention, training use and approval scope.
Oak National Academy AI tools	Teaching staff; lesson planning and curriculum support.	Exact tool and features, current terms, account requirements and data restrictions.
Canva AI	Authorised staff; educational resources and presentations.	Account and AI features, media permissions, data handling and sharing settings.
Adobe Express AI	Authorised staff; resources and communications.	Account and AI features, media permissions, data handling and sharing settings.
Purple Mash AI tools	Approved pupils and staff; curriculum activities and digital literacy.	Exact enabled features, permitted ages, supervision, filtering and data collection.
TeachMate Ai	Teaching staff and leaders; lesson planning, resource creation, assessment support, report writing and administrative tasks.	Subscription type, account ownership, permitted inputs, data retention, model training arrangements, age restrictions, safeguarding controls and approved use cases.
SLT AI	Senior leaders and authorised staff; school improvement planning, policy development, strategic analysis, communications and leadership support.	Exact product and version, licensing arrangements, data sources, permitted data categories, retention periods, training use, access controls and approval scope.
Notebook LM (Gemini)	Authorised staff; document analysis, research, summarisation, note-taking and information synthesis from approved sources.	Account type, approved data sources, sharing permissions, data retention, model training arrangements, connected services, permitted inputs and restrictions on confidential or personal data.

Tool named in previous policy	Intended users and purposes	Details to confirm
National College BlueSky AI Tools	Teaching staff, middle leaders and senior leaders; professional development support, lesson planning, resource creation, policy drafting, school improvement activities and administrative tasks.	Exact BlueSky AI tools and enabled features, subscription and licensing arrangements, account requirements, permitted data inputs, retention periods, model training arrangements, safeguarding controls, sharing permissions, data processing location, and approved use cases within the school.

Register rules

The AI Lead maintains a staff-accessible register showing active, suspended, pending and withdrawn approvals. It must identify permitted uses and data clearly. "Approved staff", "where enabled" and "approved use only" are insufficient without a defined scope. New tools, pupil access and additional data categories require a recorded decision before use.

No entry permits identifiable or confidential information unless the specific processing activity is expressly authorised under section 4. New tools must follow the same process; there is no general approval category for future products.

Appendix B Approval record

Complete one record for each tool and distinct use where the risks or permissions differ. Keep supporting documents securely and publish the operational restrictions in the staff-accessible register.

Field	Required entry or evidence
Tool and owner	Product, supplier, exact service/version or feature, school owner and contact.
Account and configuration	Licence/account type; school-managed access; connected services; enabled and disabled features; security settings.
Users and purpose	Named staff roles or pupil groups/ages; educational or operational purpose; supervision and expected benefit.
Permitted and prohibited data	Precise input/output categories, connected data and excluded information; anonymisation method where relevant.
Data protection decision	Necessity, lawful basis and additional conditions where relevant; DPO advice/date; DPIA screening outcome, DPIA reference and unresolved risks.
Supplier and retention checks	Contract/processing terms; model training; human access; subprocessors; processing locations and transfer safeguards; retention, deletion and rights handling.
Safeguarding and equality	DSL advice/date; age and account terms; filtering and monitoring; accessibility; child development and bias assessment.
Controls and evidence	Technical checks and date; test results; output review; required training; privacy notices and permissions where needed; evidence references.
Decision and conditions	Approved, pending, suspended or rejected; Headteacher name/date; authorised purposes, limits and start date.
Review and withdrawal	Review date; change triggers; incident route; person able to suspend access; exit/deletion arrangements.

Staff check before use

Check the live approval, use the correct school account, minimise information, review the complete output, and report concerns immediately. If the intended activity is outside the record, stop and ask the AI Lead before proceeding.

Appendix C Legal and guidance framework

This is a school policy supporting existing duties. It does not describe every reference below as statutory or create an exemption from legal obligations. Apply legislation as amended and in force, and the current relevant guidance. The AI Lead and DPO will check changes at adoption and review.

Legislation

Relevant legislation includes the UK General Data Protection Regulation and Data Protection Act 2018, as amended including by applicable provisions of the Data (Use and Access) Act 2025; the Education Act 2002; Equality Act 2010; Human Rights Act 1998; and Copyright, Designs and Patents Act 1988. The Online Safety Act 2023 is relevant to services within its scope; it must not be assumed to impose the same duties on every school or AI product.

Statutory safeguarding guidance

Keeping children safe in education 2026 - Department for Education

Working together to safeguard children - current edition

Government and regulator guidance

Generative artificial intelligence in education - Department for Education

Generative AI product safety standards - updated 19 January 2026

Generative AI and data protection in schools - Department for Education

Filtering and monitoring standards - Department for Education

How Ofsted looks at AI during inspection and regulation

Artificial intelligence and data protection - ICO

When a DPIA is needed - ICO

Personal data breaches - ICO

Rights and sector resources

The UN Convention on the Rights of the Child, General Comment No. 25 on children's rights in the digital environment and UNICEF's Rights Respecting Schools Award inform the school's approach. The ICO Children's Code informs assessment of relevant online services. The school may also use advice from SWGfL, UKCIS, Internet Matters, Manchester City Council, One Education and its DPO service, alongside current official guidance.