St James' Catholic Primary School

AI Policy

This policy applies to all members of the school community (including staff, learners, volunteers, parents and carers, visitors, community users) who have access to and are users of school digital systems, both in and out of the school. It also applies to the use of personal digital technology on the school site (where allowed).

Date created to replace previous Policy: 10.10.2025

Next review date: September 2026

1. Purpose & Scope

1.1. Artificial Intelligence (AI) technology is already widely used in both commercial and everyday applications, and its influence is anticipated to grow exponentially, impacting almost all industries and job sectors including education. Generative AI refers to technology that can be used to create new content based on large volumes of date that models have been trained on from a variety of works and other sources. Generative AI is a rapidly evolving and increasingly freely available technology generating writing, audio, codes, images and video simulations. Whilst this offers opportunities for schools and their pupils, it also increases risk.

1.2. AI is an integral part of the modern world and offers numerous opportunities for enhancing teaching, learning, and administrative processes. This policy establishes guidelines for the responsible and effective use of AI within our School. By embracing AI technology, we aim to:

- Enhance academic outcomes and educational experiences for pupils • Support teachers in managing their workload more efficiently and effectively
- Educate staff and pupils about safe, responsible and ethical AI use
- Incorporate AI as a teaching and learning tool to develop staff and pupils' AI literacy and skills
- Prepare staff and pupils for a future in which AI technology will be an integral part
- Promote equity in education by using AI to address learning gaps and provide personalised support
- Improve and streamline school operations to minimise cost and maximise efficiency.

1.3. All users of AI will comply with applicable laws, regulations, policies and guidelines governing Keeping Children Safe in Education, intellectual property, copyright, data protection and other relevant areas. There will be no unauthorised use of copyrighted material or creation of content that infringes on the intellectual property of others. We will prioritise the safeguarding of our pupils and their online safety and will not knowingly use any AI technology that puts their safety or privacy at risk. Staff will not allow or cause intellectual property, including pupils' work, to be used to train Generative AI models without appropriate consent or exemption to copyright.

1.4. We recognise that the technology is rapidly evolving and are committed to remaining at the forefront of developments, adapting our ways of working as necessary. We recognise the leadership in the education sector provided by the Department of Education and the guidance set out in their Statement on Generative Artificial Intelligence in Education. This AI policy has

been informed by that guidance. As guidance and technology changes the policy therefore will need to remain under regular review. This policy will therefore be reviewed annually.

1.5. We will be transparent and accountable about the use of AI technology so that stakeholders, including staff, pupils, parents and other partners understand where and how AI is used and who is responsible. Any stakeholder feedback or questions about the use of AI will be considered and responded to appropriately.

1.6 By adhering to this policy, we aim to foster a responsible and inclusive environment for the use of AI in education upholding privacy, fairness, and transparency for the benefit of all involved.

2. Legal & Policy Framework

2.1. **Statutory Safeguarding / Child Protection**

- The school will operate in line with *Keeping Children Safe in Education (KCSIE)* (currently statutory guidance) GOV.UK+2GOV.UK Assets+2
- All staff should have regard to KCSIE and specifically to sections relating to online safety, filtering/monitoring and digital risks.
- The school's Designated Safeguarding Lead (DSL) and deputies must ensure that any safeguarding concerns arising from AI/digital systems are handled in accordance with KCSIE.

2.2. **DfE Digital / Cyber Security Standards**

- The school commits to meeting the Department for Education's *Cyber Security Standards for Schools and Colleges* (as part of the broader Digital & Technology Standards) Redstor+4GOV.UK+4GOV.UK+4
- Key requirements include: governance and risk assessment, protection of devices and networks, account control, patching and software updates, backup strategy, incident reporting, and user awareness training Dataspire+3GOV.UK+3LGfL+3

2.3. **Other Relevant Requirements**

- The school will comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act in handling personal data.
- Where applicable, the school will consider relevant sector guidance (e.g. local authority ICT policies) and third-party provider SLAs through LEDS.
- The school will maintain alignment with national best practice and guidance (e.g. National Cyber Security Centre, LGfL toolkit) LGfL+2Redstor+2

3. Roles & Responsibilities

Role	Key Responsibilities in relation to AI / Digital Safety
Governing Body	Ensure adequate oversight, approve policy, ensure resources are in place to meet cyber / safeguarding obligations.
Headteacher / Senior Leadership Team (SLT)	Drive and monitor policy implementation; receive weekly safeguarding & Prevent / digital reports; ensure remedial actions are taken.
Designated Safeguarding Lead (DSL) / Deputy DSL(s)	Review digital / AI-related safeguarding incidents; escalate as needed; liaise with external agencies.
Computing Lead / Digital Lead	Oversee configuration, filtering, monitoring, security, risk assessments, and technical controls. Produce weekly reports to head/DSL.
All Staff / Volunteers	Adhere to this policy, report issues, complete training, follow AUPs and guidance on safe AI/digital usage.
Pupils	Use AI/digital systems responsibly under supervision; follow pupil AUP; report concerns to staff.
IT / Third-Party Providers (LEDS)	Configure and maintain filtering, security updates, backups, logging, and assist with incident response.

4. Use of Netsweeper Filtering & Monitoring

4.1. **Filtering & Monitoring System**

- The school uses the **Netsweeper** filtering and monitoring system to enforce acceptable use, block unsuitable or malicious content, and monitor usage logs.
- The school also uses Netsweeper+ filtering, which uses AI to monitor key strokes and online usage in real time, informing the Computing Lead and Head of any safeguarding/ prevent concerns, alongside misuse of the school's network systems.
- The filtering configuration does align with the DfE's *Filtering and Monitoring Standards* (as required under KCSIE and DfE digital guidance).
- The school will regularly review and refine filtering rules (e.g. allow vs block lists, categories, exceptions) to balance educational access and safeguarding.

4.2. **Alerting and Log Review**

- Netsweeper and Netsweeper+ is configured to generate alerts (e.g. keyword, unusual behaviour) for further investigation, in both real time and through weekly reports.
- The Computing Lead and Head (or delegated staff) will review logs and alerts daily and through weekly reports, and maintain an audit trail of investigations, actions, and outcomes.

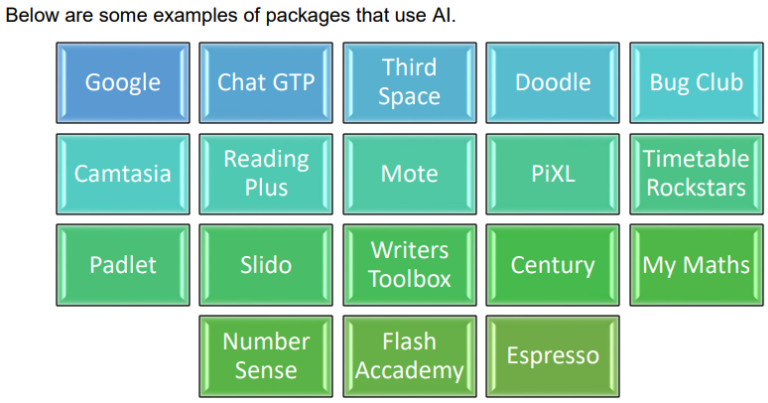
4.3. **Exception / Whitelisting / Overrides**

- Requests to override filtering (for curriculum reasons) must be approved in advance by the Computing Lead or DSL, logged and time-limited.
- Overrides will be documented, with justification, duration, and returned to normal settings once no longer needed.

5. AI / Generative Tools: Acceptable Use & Safeguards

5.1. **Definition**

- For this policy, "AI tools" refer to generative AI (e.g. language models, image generation, code generation) and any system employing automated inference or decision support.



5.2. **Permitted Uses**

- AI tools may be used to support teaching, learning, research, planning, and administrative tasks, provided there is oversight, validation, and alignment with pedagogical aims.
- Pupils may use AI under supervision, with clear instruction, scaffolded tasks, and emphasis on critical thinking, attribution, and verification.

5.3. **Prohibited / Risk Areas**

- Use of AI to generate inappropriate or harmful content (e.g. misinformation, disinformation, extremist materials) is prohibited.
- Pupils must not use AI to generate abusive, harassing, or plagiarised work.
- Sensitive personal or safeguarding data must not be input into third-party AI services without proper anonymisation and data protection safeguards.

5.4. **Review & Verification**

- Outputs from AI tools must be reviewed by a human (teacher / staff) before dissemination or student use.
- AI-generated material used in school resources should be clearly labelled, and the provenance/context explained to pupils.

5.5. **Training & Guidance**

- Staff must undertake training on safe and effective use of AI tools (benefits, limitations, risks).
- The school should provide pupils with guidance on AI literacy, including how to question, verify, and critique AI outputs.

6. Safeguarding Reporting: Weekly Reports & Escalation

6.1. **Weekly Safeguarding / Digital Safety Report**

- The Computing Lead (or designated staff) will compile a weekly safeguarding / digital safety report, summarising:
    - Netsweeper alerts triggered / flagged incidents
    - Investigations conducted, outcomes, follow up actions
    - Requests for filtering overrides or exceptions
    - Addition of devices to the school's network and filtering system
    - Outcomes of monitoring on the system or adaptations made
    - Any near misses, suspicious behaviours, or concerns
    - Trends or emerging risks (e.g. repeated attempts at accessing blocked content)
- This weekly report is copied to the Headteacher, DSL, and Computing Lead for review.

6.2. **Prevent / Extremism Reports**

- If the filtering / monitoring system or staff identify content or behaviours linked to radicalisation, extremism or terrorism (i.e. "Prevent" relevant), a separate Prevent Report is prepared and submitted weekly to the Headteacher and DSL (or Computing Lead if delegated).
- Such reports will include: user, content flagged, context, actions taken, referrals made (where applicable).

6.3. **Escalation & Action**

- The Headteacher, DSL, and Computing Lead will review the weekly reports, determine if further safeguarding referral or disciplinary action is needed.
- Trends or recurring issues must trigger a review of filtering rules, staff training, or policy amendments.

- Significant safeguarding incidents must be escalated immediately (not waiting for weekly batch reports) to DSL, external agencies (e.g. social care, police) as required under KCSIE.

7. Risk Assessment, Monitoring & Review

7.1. **Cyber / AI Risk Assessment**

- The school will maintain a formal AI / digital risk register and conduct a full cyber risk assessment annually (and review termly).
- The risk assessment should cover: filtering gaps, user account security, third-party AI tools, data classification, potential misuse, incident response capability.

7.2. **Policy Review**

- This AI & Digital Safety Policy will be reviewed annually (or sooner in response to incidents or guidance changes) by SLT, DSL, governors, computing lead, and IT provider.

7.3. **Auditing & Penetration Testing**

- The school should periodically (e.g. annually or biannually) commission external auditing / penetration testing of its network, filtering, cloud services, and digital infrastructure.

8. Incident Response & Breach Protocols

8.1. **Incident Classification & Logging**

- Any breach, cybersecurity incident, or misuse of AI (e.g. generation of harmful content, data leak) must be logged in the school's incident log, classified (e.g. low, medium, high), and escalated in line with the school's Incident Response Plan.

8.2. **Notification & Reporting**

- The school will follow the DfE Cyber Security Standards guidance for reporting cyber attacks or breaches internally and externally Redstor+3GOV.UK+3files.anme.co.uk+3
- Where personal data is involved, the school must assess whether a notifiable data breach must be made to the Information Commissioner's Office (ICO).
- If required, report to external agencies (e.g. Action Fraud, DfE) as per DfE standards files.anme.co.uk+2GOV.UK+2

8.3. **Containment, Recovery & Learning**

- The computing / IT team should act quickly to contain the incident, restore systems from backups, secure vulnerabilities, and document lessons learned.
- Post-incident, the school should hold a review meeting (SLT, computing lead, safeguarding lead) to adjust policies, training, or technical controls.

9. Training, Awareness & Culture

9.1. **Staff Training**

- Annual (or more frequent) training on digital safety, AI risks, filtering / monitoring alerts, phishing, account security, incident reporting, and policy responsibilities.
- New staff / volunteers will receive induction on this AI & Digital Safety Policy and associated procedures.

9.2. **Pupil Education**

- The school will embed digital literacy and AI awareness in the curriculum (age-appropriate).
- Pupils should be taught how to use AI tools responsibly, understand limitations, recognise misinformation, and report concerns.

9.3. **Parental Engagement & Communication**

- The school will inform parents about the use of AI tools, filtering practices, and expectations of pupil conduct, through the acceptable use agreement and periodic communication.
- Provide guidance for safe home use of AI / internet, including use of parental controls.

10. Acceptable Use & Sanctions

10.1. **Integration with AUPs**

- This policy's rules augment, not replace, the school's existing Acceptable Use Policies for staff, pupils, and visitors.
- AI / digital tool use should be explicitly referenced in those AUPs, with clear expectations and restrictions.

10.2. **Sanctions & Remediation**

- Breaches of this policy (e.g. misuse of AI, circumventing filters, generating harmful content) will be dealt with in accordance with the school's behaviour / disciplinary policies, and may include withdrawal of digital privileges, intervention, parental involvement, or further sanctions.

- Where breaches reveal gaps in training or filtering, remedial training or system adjustments must follow.

Acceptable use

The school has defined what it regards as acceptable/unacceptable use and this is shown in the tables below.

Acceptable use agreements

The Online Safety Policy and acceptable use agreements define acceptable use at the school. The acceptable use agreements will be communicated/re-enforced through:

- staff induction and handbook
- digital signage
- posters/notices around where technology is used
- communication with parents/carers
- built into education sessions
- school website

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not access online content (including apps, games, sites) to make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	**Any illegal activity for example:** • Child sexual abuse imagery* • Child sexual abuse/exploitation/grooming • Terrorism • Encouraging or assisting suicide • Offences relating to sexual images i.e., revenge and extreme pornography • Incitement to and threats of violence • Hate crime • Public order offences - harassment and stalking • Drug-related offences • Weapons / firearms offences					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
	• Fraud and financial crime including money laundering N.B. Schools should refer to guidance about dealing with self-generated images/sexting – UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in schools and colleges					
Users shall not undertake activities that might be classed as cyber-crime under the Computer Misuse Act (1990)	• Using another individual's username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised) • Gaining unauthorised access to school networks, data and files, through the use of computers/devices • Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g., financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission) N.B. Schools will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. The National Crime Agency has a remit to prevent learners becoming involved in					X

User actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
	cyber-crime and harness their activity in positive ways– further information here					
Users shall not undertake activities that are not illegal but are classed as unacceptable in school policies:	Accessing inappropriate material/activities online in a school setting including pornography, gambling, drugs. (Informed by the school's filtering practices and/or AUAs)			X	X	
	Promotion of any kind of discrimination				X	
	Using school systems to run a private business				X	
	Using systems, applications, websites or other mechanisms that bypass the filtering/monitoring or other safeguards employed by the school				X	
	Infringing copyright				X	
	Unfair usage (downloading/uploading large files that hinders others in their use of the internet)			X	X	
	Any other information which may be offensive to others or breaches the integrity of the ethos of the school or brings the school into disrepute				X	

When using communication technologies, the school considers the following as good practice:

- when communicating in a professional capacity, staff should ensure that the technologies they use are officially sanctioned by the school.
- any digital communication between staff and learners or parents/carers (e-mail, social media, learning platform, etc.) must be professional in tone and content.

Personal e-mail addresses, text messaging or social media must not be used for these communications.

- staff should be expected to follow good practice when using personal social media regarding their own professional reputation and that of the school and its community
- users should immediately report to a nominated person – in accordance with the school policy – the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- *relevant policies and permissions should be followed when posting information online e.g., school website and social media. Only school e-mail addresses should be used to identify members of staff and learners.*