

Artificial Intelligence (AI) and Online Safety Policy

1. Purpose

The school is committed to providing a safe, secure, and positive learning environment for all students and staff. As Artificial Intelligence (AI) technologies become increasingly accessible, this policy outlines the safe, ethical, and responsible use of AI and online technologies while ensuring the safeguarding and wellbeing of all members of the school community.

2. Scope

This policy applies to:

- All students
 - All staff, contractors, and volunteers
 - Parents and carers when engaging with school digital platforms
 - All AI-enabled technologies used within school systems, devices, networks, and learning environments
-

3. Guiding Principles

The school will:

- Prioritise the safety and wellbeing of students.
- Promote responsible and ethical use of AI technologies.
- Protect personal data and privacy.
- Ensure AI tools are used to enhance learning while maintaining appropriate human oversight.
- Respond promptly and effectively to safeguarding concerns involving AI.

4. Safeguarding Risks Associated with AI

4.1 AI-Generated Abuse

AI technologies can be misused to create:

- Deepfake images and videos.
- Voice cloning and impersonation.
- Manipulated content designed to humiliate, threaten, bully, or exploit others.
- Sextortion attempts using AI-generated or altered content.

Such behaviour may constitute bullying, harassment, abuse, or criminal activity and will be treated as a serious safeguarding concern.

4.2 Exposure to Harmful or Inappropriate Content

AI tools may generate or surface content that is:

- Violent
- Sexual or explicit
- Discriminatory or hateful
- Misleading or harmful

Students may intentionally or unintentionally access inappropriate material through AI platforms. Appropriate filtering, monitoring, and supervision must be maintained.

4.3 AI Chatbots and AI Companions

AI chatbots and companion applications can:

- Simulate personal relationships.
- Encourage excessive or unhealthy engagement.
- Provide inaccurate, inappropriate, or dangerous advice.
- Distort reality or create emotional dependency.

Students should understand that AI systems are not human, do not replace trusted adults, and should never be relied upon for personal, medical, emotional, or safeguarding advice.

4.4 Data Privacy and Surveillance Risks

AI systems often collect and process significant amounts of data.

Potential risks include:

- Unauthorised sharing of personal information.
- Inappropriate collection of student data.
- Third-party access to sensitive information.
- Data breaches and privacy violations.

All AI platforms used within school must comply with applicable data protection legislation and school data privacy requirements.

5. Safe Use of AI

Staff Responsibilities

Staff must:

- Use only approved AI tools for educational purposes.
 - Maintain professional judgement and human oversight.
 - Verify AI-generated information before sharing it with students.
 - Avoid entering confidential, sensitive, or personally identifiable student information into AI systems unless explicitly approved.
 - Supervise student use of AI technologies.
 - Report safeguarding concerns immediately.
-

Student Responsibilities

Students must:

- Use AI tools only for approved educational purposes.
- Treat others respectfully online and when using AI.
- Never create, share, or distribute harmful AI-generated content.
- Never use AI to impersonate another person.

- Report any concerning AI-generated content, messages, or interactions.
 - Protect personal information and the privacy of others.
-

6. Prevention Measures

The school will:

Technology Controls

- Use AI platforms with strict content filters and age-appropriate settings.
- Ensure appropriate filtering and monitoring systems are in place.
- Restrict access to unapproved AI applications where appropriate.

Supervision

- Supervise AI use in classrooms and learning environments.
- Restrict unsupervised student access to AI technologies.
- Maintain active staff vigilance during AI-related activities.

Education and Awareness

- Educate students about AI-enabled abuse, including deepfakes, voice cloning, impersonation, and sextortion.
- Promote online skepticism and critical thinking.
- Encourage students to question the authenticity of digital content and communications.
- Teach students how to verify information before acting upon it.

Digital Citizenship

The school will educate students about:

- Privacy and data protection.
- Respectful online behaviour.
- Responsible use of AI technologies.
- Digital footprints and reputation.
- The risks and consequences of sharing explicit or personal content online.

Reporting Culture

The school will:

- Ensure students know how to report concerns.
 - Foster an environment where students feel safe seeking help.
 - Promote trusted adult support both within and outside school.
-

7. Responding to AI-Related Safeguarding Concerns

Any AI-related safeguarding concern must be treated seriously.

Examples include:

- Deepfake images or videos involving students or staff.
- AI-generated bullying or harassment.
- Sextortion attempts.
- Voice cloning or impersonation.
- Harmful chatbot interactions.
- Exposure to inappropriate AI-generated content.
- Privacy or data protection concerns.

Immediate Actions

When an AI-related safeguarding concern is identified:

1. Immediately inform the IT Department and Designated Safeguarding Lead (DSL).
2. Preserve available evidence where appropriate and safe to do so.
3. Log the incident on GUARD.
4. Assess immediate risk to the student(s) involved.
5. Follow the school's safeguarding procedures.
6. Contact external agencies where required.
7. Offer pastoral support to affected students.

8. Data Protection

The school will:

- Minimise data sharing with AI providers.
 - Regularly review AI systems used within the school.
-

9. Staff Training

The school will provide regular training on:

- Safe and effective use of AI.
 - AI-related safeguarding risks.
 - Deepfakes, sextortion, and impersonation.
 - Data protection and privacy.
 - Reporting and responding to concerns.
-

10. Monitoring and Review

This policy will be reviewed annually or sooner if:

- New safeguarding guidance is issued.
- Significant technological developments occur.
- Serious incidents indicate the need for revision.

The school leadership team and Designated Safeguarding Lead will oversee implementation and review.

Last review: 2/6/2026