

AI, Digital Technology and Online Safety Policy



**Burwell Village
College Primary**

Approved by:	Governing Body	Date: February 2021
Last reviewed on:	October 2026	
Next review due by:	October 2029	

Burwell Village College Primary School

AI, Digital Technology and Online Safety Policy

Approved by Governing Body | Review Cycle: Annual | Applies to all staff, pupils, governors, volunteers and visitors

1. Purpose and Scope

This policy establishes the school approach to the safe, ethical and effective use of artificial intelligence (AI), digital technology and online services. The school recognises that AI can improve productivity, accessibility and learning opportunities; however, it also introduces safeguarding, privacy, misinformation and cyber-security risks. This policy sets out the standards expected of all members of the school community. The policy applies to the use of school-owned devices, personal devices used for school purposes, cloud services, AI systems, online platforms and any technology used to support teaching, learning or school operations.

Implementation expectations: leaders will evidence compliance through audits, training records, curriculum monitoring, safeguarding reviews, governor scrutiny and documented actions.

2. Core Principles

The school will place child safety before technological innovation. Human judgement remains responsible for all decisions affecting children.

- AI outputs must be reviewed before use.
- Personal data will be protected.
- The school will encourage digital literacy, critical thinking and responsible technology use.
- Equality, inclusion and accessibility will be considered in all technology decisions.

Implementation expectations: leaders will evidence compliance through:

- audits,
- training records,
- curriculum monitoring,
- safeguarding reviews,
- governor scrutiny
- documented actions.

3. Legislative Framework

This policy should be read alongside safeguarding, behaviour, staff conduct and data protection policies. School leaders will ensure that AI and online safety arrangements remain consistent with statutory safeguarding guidance, data protection requirements and Department for Education expectations.

4. Roles and Responsibilities

Governors provide strategic oversight and challenge.

The Headteacher is responsible for implementation.

The Designated Safeguarding Lead oversees AI-related safeguarding concerns, online incidents and referrals.

The Data Protection Officer advises on privacy and data protection risks.

The Computing Lead supports curriculum implementation.

All employees have a responsibility to report concerns immediately and to follow this policy at all times.

5. Governance of AI

No AI tool should be adopted solely because it is popular or widely available. Before implementation the school will consider safeguarding implications, minimum age requirements, privacy notices, contractual arrangements, cyber-security controls, record retention, accessibility and educational value. A register of approved AI tools will be maintained and reviewed annually.

6. Staff Use of AI

Appropriate staff use includes supporting lesson planning, creating draft communications, developing resources, adapting materials for pupils with SEND, generating administrative summaries and supporting professional development. Staff must always verify facts, review quality and ensure content is suitable for pupils. AI must never make safeguarding decisions, disciplinary decisions, recruitment decisions or professional judgements. Confidential pupil information must not be entered into unauthorised systems.

7. Pupil Use of AI

Pupils may access AI-enabled tools only when approved by the school and under suitable supervision. Teaching will focus on understanding limitations, recognising inaccurate information, questioning sources and using technology responsibly. Pupils should understand that AI-generated content may be incorrect, biased or misleading. Independent thinking remains essential.

8. Curriculum

Online safety and AI literacy will be integrated through computing and PSHE. Other curriculum subjects can be utilised where useful and appropriate, for example writing about the dangers of online content. Pupils will learn about digital footprints, privacy, misinformation, disinformation, algorithms, deepfakes, cyberbullying, online relationships, copyright and responsible participation in digital environments.

9. Safeguarding

AI-related safeguarding concerns include grooming, exploitation, radicalisation, cyberbullying, harassment, extremism, self-harm content, synthetic media and impersonation. Any concern involving a child must be reported immediately through safeguarding procedures. Delays in reporting are unacceptable. Records will be maintained using established safeguarding systems, in our school this is MyConcern.

10. Deepfakes and Synthetic Content

Images, video or audio generated or altered using AI can create significant safeguarding risks. The creation, possession or sharing of harmful AI-generated content involving children will be treated seriously. Staff must never investigate potentially illegal images independently. Concerns must be referred immediately to the DSL who will determine appropriate safeguarding actions and external referrals.

Images of children can be used with parental permission in different contexts for example, the local newspaper and the school website. The school makes clear what these images will be used for.

11. Filtering and Monitoring

The school will maintain proportionate filtering and monitoring arrangements. Leaders will review effectiveness every term in discussion with the relevant system providers. This will form part of the safeguarding report by the safeguarding governor supported by the online safety lead governor. Leaders will consider emerging technologies and ensure systems support safeguarding practice. Alerts and incidents will be reviewed promptly and acted upon where necessary.

12. Data Protection and Privacy

Only approved systems may process personal data. Staff must consider data minimisation, lawful basis, retention, security and confidentiality. Where required, leaders will complete a Data Protection Impact Assessment before implementation of new services. Suppliers should provide appropriate assurance around security and privacy.

13. Cyber Security

Strong passwords, multifactor authentication where available, software updates, secure storage and phishing awareness are essential expectations. Suspected cyber incidents must be reported immediately. Staff should remain alert to AI-enabled phishing attacks and social engineering attempts.

14. Copyright and Intellectual Property

Staff and pupils should respect intellectual property rights and licensing conditions. AI-generated content may not be free from copyright restrictions. Sources should be checked and appropriately acknowledged where required.

15. Assessment and Academic Integrity

AI may support learning but should not undermine assessment integrity. Teachers will make clear when independent work is required. Pupils should be taught how to acknowledge appropriate technological support and understand the importance of authentic learning.

16. Staff Training

All staff will receive online safety and AI awareness training. Training will include privacy, misinformation, safeguarding risks, deepfakes, cyber-security, acceptable use and incident reporting. New employees will receive basic induction training before accessing school systems.

17. Parental Engagement

The school will provide information to parents about online safety, social media, gaming, AI tools and emerging digital risks. Parents will be encouraged to discuss technology use at home and seek support where concerns arise.

Parents are able to record school events but these are for personal use only. No images of children should be shared on social media. If breaches of this policy occur the individual parent may have permission revoked or they may be removed from other school events. If persistent or widespread breaches occur the school may choose to stop all recording of school events.

18. Incident Response

Incidents will be reported, recorded, investigated and resolved proportionately. Significant incidents will be reviewed to identify lessons learned. Where required, external agencies will be contacted and appropriate records retained.

19. Monitoring and Review

Governors will receive termly reports regarding safeguarding incidents, filtering and monitoring effectiveness and implementation progress. This policy will be reviewed annually or earlier if significant legislative or technological changes occur.