Aston Rowant C†E Primary School

Digital Learning, IT and Online Safety Policy

Vision: To be a community of courageous life-long learners, who are rooted in God, live out our Christian values and enjoy life in all its fullness. *(Col 2:1-7)*
Mission: Growing together, rooted in God and inspiring one another through our values and our broad enriched curriculum.
Strapline: Growing together, rooted in God, having fullness of life *(Col 2:1-7)*

Our Digital Learning, IT & Online Safety Policy is grounded in our Christian ethos, recognising every child as uniquely created, precious and deserving of safety, empowerment and opportunity. This policy supports our responsibility to safeguard, educate and equip pupils to flourish in an increasingly digital world.

Linked Policies

- Safeguarding & Child Protection Policy
- Behaviour Policy
- Anti-Bullying Policy
- Data Protection Policy
- Mobile Phone Policy
- Acceptable Use Agreements
- Staff Code of Conduct
- KCSIE

1. Purpose of the Policy

This policy consolidates all aspects of digital provision within the school, including:

- Computing curriculum implementation
- Digital learning and digital literacy
- Online safety as part of safeguarding
- Acceptable Use expectations for staff, pupils, governors and parents
- Infrastructure, filtering, monitoring and data protection
- Device management and mobile phone expectations
- Roles, responsibilities and leadership oversight

It ensures a consistent, whole-school approach in line with the **National Curriculum**, **KCSIE 2025**, **Data Protection legislation**, and the **Education for a Connected World (DfE)** framework.

2. Curriculum Intent

Our Computing and digital learning curriculum aims to:

- Develop resilient, creative, logical learners able to use technology confidently
- Equip pupils with essential skills in computer science, information technology and digital literacy
- Teach children to behave safely, responsibly and respectfully online
- Provide equal access to high-quality resources across all year groups
- Inspire curiosity, problem-solving and collaboration

We use the Kapow Primary Computing Scheme, ensuring progression, vocabulary development and alignment to statutory requirements.

3. Implementation

3.1 Teaching & Learning

Pupils access a rich computing curriculum using:

- Two laptop trolleys
- Two iPad trolleys
- Bee-Bots (KS1)
- Micro:bits and codable robots (KS2)
- Interactive whiteboards
- Cameras, visualisers, microphones and sound systems
- VR headsets (via hire) to enrich curriculum learning

Teachers plan purposeful, meaningful digital experiences using high-quality resources.

3.2 Cross-Curricular Digital Learning

Technology supports learning across all subjects, including:

- Research
- Presenting information
- Digital creativity
- Data collection
- Publishing
- Video and audio production

This supports children's preparation for the digital future.

4. Impact

We measure success through:

- Pupil voice and digital confidence
- Work scrutiny and digital portfolios
- Progression against Kapow outcomes
- Safe and responsible online behaviours
- Reduction in digital safeguarding incidents
- Staff confidence and training records

5. Online Safety

Online safety is a core safeguarding priority and forms part of the school's wider safeguarding arrangements. It directly aligns with Keeping Children Safe in Education (KCSIE) and is embedded throughout the curriculum.

We follow the Education for a Connected World framework, ensuring progression in:

- Self-image & identity
- Online relationships
- Online reputation
- Online bullying
- Managing information
- Health, wellbeing & lifestyle
- Privacy & security
- Copyright & ownership

5.1 Annual Safer Internet Day

We participate every February, using national themes to deepen understanding through assemblies, workshops, discussions, parent communications and classroom activities.

5.2 Teaching Children to Be Safe Online

Pupils learn to:

- Recognise risks and respond appropriately
- Report concerns to trusted adults
- Communicate safely and respectfully
- Protect personal information
- Understand reliability, bias and misinformation
- Recognise the permanence of digital footprints
- Be resilient, kind and responsible digital citizens

5.3 Monitoring & Filtering

We use approved school filtering and monitoring systems in line with DfE guidance, overseen by:

- The Headteacher (DSL)
- The Online Safety Lead
- Governors

6. Roles & Responsibilities

6.1 Governing Body

- Ensures the school meets statutory online safety and IT requirements
- Reviews policies, monitoring reports and safeguarding updates

6.2 Headteacher / Designated Safeguarding Lead

- Holds strategic oversight of digital safeguarding
- Ensures compliance with KCSIE and statutory duties
- Oversees CPD, policies and incident management

6.3 Online Safety Lead / Computing Lead

- Develops and reviews digital strategy
- Ensures curriculum coverage
- Oversees filtering, monitoring and incident response
- Leads staff training

6.4 Staff

All staff must:

- Model safe, respectful, responsible behaviour
- Complete Online Safety training
- Report concerns immediately
- Follow Acceptable Use Agreements
- Safeguard pupils in line with KCSIE

6.5 Pupils

Pupils must:

- Use technology with care and respect
- Follow Acceptable Use rules
- Report concerns or unsafe behaviour
- Protect their login details and personal information

6.6 Parents & Carers

- Support safe digital behaviour at home
- Engage with workshops, updates and Acceptable Use expectations
- Report concerns promptly

7. Acceptable Use

7.1 Staff AUP

Staff must:

- Use school systems professionally
- Keep data safe
- Use only school email for school business
- Follow safeguarding principles, including those in KCSIE
- Maintain professional boundaries online
- Never share pupil images on personal devices

7.2 Pupil AUP

Pupils must:

- Use devices safely and sensibly
- Ask permission before going online
- Use only their own accounts
- Never share personal information
- Report concerns immediately

7.3 Parent AUP

Parents must:

- Support the school's online safety expectations
- Model safe digital behaviours
- Not share images of other children without consent
- Communicate with staff via official channels

8. Mobile Phones, Smart Watches & Devices

Aligned with DfE non-statutory guidance (2024/2026), the school is a mobile-phone-free environment for pupils.

- Phones brought for travel must be handed in on arrival
- Smart watches with cameras/internet must be handed in
- Non-connected watches may be worn as timepieces only
- Misuse will result in confiscation and parental collection

9. Loan Devices

Loan agreements exist for:

- Pupils
- Staff

These must be signed and followed fully. Devices remain school property.

10. Data Protection

The school follows:

- UK GDPR
- Data Protection Act 2018
- School Data Protection Policy

Personal data must only be stored, transferred and accessed securely.

11. Managing Emerging Technologies

All emerging technologies will be risk-assessed before use. Staff must not introduce new software, apps or programmes without approval.

This includes:

- AI tools
- VR
- Robotics
- New communication platforms

Use will always prioritise safeguarding and pedagogy.

12. Incident Management

- All concerns must be reported to the DSL
- DSL records incidents securely
- Serious digital safeguarding concerns follow child protection procedures
- Governors receive anonymised oversight

13. Monitoring the Effectiveness of this Policy

The school monitors:

- Incident logs
- Filtering alerts
- Pupil voice
- Staff CPD
- Curriculum coverage
- Safeguarding audits

This policy will be reviewed at least every two years