CITY OF BIRMINGHAM EDUCATION DEPARTMENT

BASKERVILLE SCHOOL

e-SAFETY POLICY

BASKERVILLE SCHOOL E-SAFETY POLICY
Date reviewed: September 2025
Next review: September 2026
Headteacher: Allan Lacey
Baskerville School
Fellows Lane, Harborne, Birmingham, B17 9TS
Telephone: 0121 427 3191
Email: enquiries@baskvill.bham.sch.uk

VISION STATEMENT
To provide an outstanding, inclusive educational provision to prepare students for a fulfilled life.

---

1. INTRODUCTION AND OVERVIEW

1.1 Purpose and Rationale

This policy sets out Baskerville School's approach to online safety (e-safety) and establishes clear expectations for the safe and responsible use of digital technologies by all members of our school community.
All students at Baskerville School have autism spectrum conditions, which means they may face additional challenges with social understanding and communication. This policy recognises both the significant benefits that digital technologies offer our students and the vulnerabilities they may face online.

1.2 Key Benefits for Students with Autism

Digital technologies provide valuable opportunities for our students:

- **Communication support** - Online platforms use consistent emoticons and visual cues, reducing the need to interpret complex facial expressions and vocal tones
- **Learning reinforcement** - Internet-based learning allows for repetition and practice at the student's own pace
- **Social interaction** - Structured online environments can provide safe spaces for social communication
- **Independence** - Digital tools can support daily living skills and future employment opportunities

1.3 Recognised Risks

Alongside these benefits, we acknowledge that students with autism may face heightened risks online due to:

- Increased vulnerability to exploitation
- Tendency towards obsessive or compulsive behaviours
- Social naivety and difficulty recognising deception
- Challenges in understanding consequences of actions

1.4 Scope of this Policy

This policy applies to all members of the Baskerville School community, including:

- Students
- Staff (teaching and support)
- Governors
- Volunteers
- Visitors
- Parents and carers

The policy covers the use of all digital technologies both on school premises and when used in connection with the school community off-site.

---

2. LEGAL FRAMEWORK AND RELATED POLICIES

This policy has been developed in accordance with current UK legislation and statutory guidance including:

Key Legislation:

- Online Safety Act 2023 (fully in force from 2025)
- UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018
- Data (Use and Access) Act 2025

- Education Act 2002 and 2011
- Children Act 1989 and 2004
- Computer Misuse Act 1990
- Communications Act 2003
- Equality Act 2010

Statutory Guidance:

- Keeping Children Safe in Education (KCSIE) 2025
- Working Together to Safeguard Children 2023
- Filtering and Monitoring Standards for Schools (DfE 2024)

Related School Policies:

1. Safeguarding and Child Protection Policy
2. Behaviour Policy
3. Anti-Bullying Policy
4. Staff Code of Conduct
5. Acceptable Use Agreements (Staff and Students)
6. Mobile Phone Policy
7. Data Protection Policy
8. PSHE and RSE Policy
9. Special Educational Needs and Disabilities (SEND) Policy
10. Alternative Provision Policy

---

3. ROLES AND RESPONSIBILITIES

3.1 Headteacher - Allan Lacey

Key responsibilities:

- Overall accountability for online safety provision and compliance with the Online Safety Act 2023
- Acting as Senior Information Risk Officer (SIRO) under UK GDPR requirements
- Ensuring compliance with KCSIE 2025 statutory obligations
- Ensuring staff receive appropriate training on online safety and data protection (minimum every two years)
- Maintaining awareness of current online safety issues and emerging technologies
- Ensuring appropriate filtering and monitoring systems meet DfE standards
- Reporting significant incidents to governors, local authority, and Ofcom where required
- Ensuring school meets Online Safety Act duties of care for protecting children online

3.2 E-Safety Coordinator (Assistant Head - Pastoral)

Key responsibilities:

- Day-to-day management of e-safety
- Developing and reviewing e-safety policies
- Coordinating e-safety education across the curriculum
- Maintaining incident logs and reporting systems
- Liaising with external agencies
- Training and supporting staff
- Regular communication with senior leadership and governors

3.3 Designated Safeguarding Lead

Key responsibilities:

- Handling e-safety incidents with safeguarding implications

- Reporting serious incidents to Children's Services and Police
- Maintaining awareness of online risks to vulnerable young people
- Training staff on safeguarding aspects of e-safety

3.4 Computing Curriculum Leader

Key responsibilities:

- Ensuring e-safety is embedded in computing curriculum
- Supporting colleagues with technical e-safety issues
- Keeping up to date with technological developments

3.5 Network Manager/ICT Technician

Key responsibilities:

- Maintaining secure network infrastructure
- Implementing and monitoring filtering systems
- Regular security updates and virus protection
- Managing user access and passwords
- Reporting technical security incidents
- Secure data backup and recovery procedures

3.6 Teaching Staff

Key responsibilities:

- Embedding e-safety in curriculum delivery
- Supervising students' technology use
- Modelling safe digital behaviour
- Reporting concerns immediately
- Maintaining professional boundaries in digital communications
- Following acceptable use agreements

3.7 All Staff

Key responsibilities:

- Following school e-safety policies
- Maintaining awareness of current risks
- Reporting incidents and concerns
- Professional use of technology
- Supporting students' safe technology use

3.8 Students

Key responsibilities:

- Following acceptable use agreements
- Reporting concerns to trusted adults
- Respecting others online
- Protecting personal information
- Understanding consequences of inappropriate behaviour

3.9 Parents and Carers

Key responsibilities:

- Supporting school e-safety policies
- Discussing online safety at home
- Monitoring their child's internet use
- Reporting concerns to school
- Engaging with school communications about e-safety

3.10 Governors

Key responsibilities:

- Strategic oversight of e-safety provision
- Ensuring policy compliance
- Supporting staff development

- Regular review of incidents and procedures

---

4. E-SAFETY EDUCATION AND CURRICULUM

4.1 Student E-Safety Education

Our progressive e-safety programme is embedded within Computing and PSHE curricula, covering age-appropriate skills and knowledge including:

Foundation Skills:

- STOP and THINK before you CLICK
- Recognising reliable information sources
- Understanding author bias in online content
- Effective search strategies
- Understanding how search engines work

Communication and Behaviour:

- Appropriate online behaviour and language
- Keeping personal information private
- Understanding digital footprints
- Email etiquette and safety

Critical Thinking and Digital Literacy:

- Identifying manipulated images and deepfake content
- Recognising misinformation, disinformation, and conspiracy theories
- Understanding algorithmic bias and filter bubbles
- Evaluating website credibility and fact-checking
- Understanding the commercial nature of online platforms

Emerging Technology Awareness:

- Safe use of generative AI and chatbots
- Understanding AI-generated content
- Implications of biometric data collection
- Internet of Things (IoT) device security
- Virtual and augmented reality safety

Safety Awareness:

- Recognising and responding to cyberbullying
- Understanding the risks of sharing personal content
- Safe social media practices
- Privacy settings and digital reputation
- Seeking help for online problems

Legal and Ethical Issues:

- Copyright and intellectual property
- Consequences of inappropriate behaviour
- Understanding terms and conditions
- Digital citizenship responsibilities

4.2 Staff Training and Development

All staff receive regular e-safety training covering:

- Current online risks and trends
- School policies and procedures
- Recognising signs of online abuse
- Professional use of technology
- Supporting students with autism online
- Incident reporting procedures

4.3 Parent and Carer Engagement

We provide ongoing support to families through:

- Information sessions on online safety
- Resources for home internet safety
- Guidance on parental controls
- Regular updates on current risks
- Support for families experiencing difficulties

---

5. TECHNICAL INFRASTRUCTURE AND SECURITY

5.1 Internet Access and Filtering

Our systems comply with DfE Filtering and Monitoring Standards 2024 and include:

- Secure filtered internet connection via DfE-approved provider
- Age-appropriate content filtering that meets Ofcom standards
- Blocked access to illegal content as defined by the Online Safety Act 2023
- Protection from content harmful to children including:
  - Pornographic content with robust age verification
  - Self-harm, suicide, and eating disorder content
  - Bullying and hateful content
  - Content encouraging dangerous behaviours
- Educational exceptions for legitimate research with appropriate safeguards
- Real-time monitoring and logging of internet usage
- Advanced virus protection and malware scanning
- Regular assessment and review of filtering effectiveness

5.2 Network Security

Security measures under UK GDPR and Data (Use and Access) Act 2025:

- Individual password-protected accounts for all users with strong password policies
- Multi-factor authentication where technically feasible
- Regular password changes (every 90 days for staff, 180 days for students)
- Encrypted data storage and transmission
- Secure backup procedures with off-site storage
- Restricted administrative access with audit trails
- Regular security updates and vulnerability assessments
- Intrusion detection and prevention systems

5.3 Email Systems

Email safety measures:

- School-provided email accounts for professional use
- Spam and phishing protection
- Restrictions on external email for students
- Monitoring of email communications
- Clear guidance on appropriate use

5.4 Data Protection and Privacy

Compliance with UK GDPR, Data Protection Act 2018, and Data (Use and Access) Act 2025:

- Data Protection Impact Assessments (DPIAs) for all new systems
- Privacy by design principles embedded in all technology decisions
- Regular data audits and retention schedule compliance
- Secure data sharing protocols with appropriate legal basis
- Subject access request procedures with "stop the clock" provisions

- Personal data breach notification within 72 hours to ICO where required
- Annual data protection training for all staff
- Privacy notices regularly reviewed and updated
- Automated decision-making safeguards where applicable

5.5 Online Safety Act 2023 Compliance

Platform and service provider oversight:

- Regular assessment of third-party platforms used by the school
- Ensuring providers meet their duties under the Online Safety Act
- Reporting mechanisms for platform non-compliance to Ofcom
- Due diligence on age assurance measures for platforms
- Monitoring compliance with children's safety codes of practice

---

6. ACCEPTABLE USE AND CONDUCT

6.1 General Principles

All users must:

- Use technology responsibly and safely
- Respect others' rights and privacy
- Follow school policies and legal requirements
- Report inappropriate behaviour or content
- Maintain appropriate professional/personal boundaries

6.2 Prohibited Activities

The following activities are strictly forbidden:

- Accessing inappropriate or illegal content
- Cyberbullying or online harassment
- Sharing personal information inappropriately
- Downloading unauthorised software or media
- Attempting to bypass security measures
- Using technology for commercial purposes
- Plagiarising or violating copyright

6.3 Student Guidelines

Students must:

- Only use school accounts and approved platforms
- Keep passwords confidential
- Report uncomfortable or inappropriate interactions
- Seek permission before sharing images or videos
- Follow teacher instructions for technology use
- Use appropriate language in all communications

6.4 Staff Guidelines

Staff must:

- Use school-provided accounts for professional communications
- Maintain clear boundaries with students online
- Report all safeguarding concerns immediately
- Model appropriate digital behaviour
- Follow data protection requirements
- Document home communications appropriately

---

7. MOBILE DEVICES AND PERSONAL TECHNOLOGY

7.1 Student Mobile Phones

- Mobile phones must be switched off or silent during school hours
- Phones must be stored securely during lessons

- Use only permitted during breaks with staff supervision
- Recording (photo, video, audio) is prohibited without explicit permission
- Confiscation procedures apply for policy breaches

7.2 Staff Personal Devices

- Personal devices must not be used to contact students
- School-provided devices must be used for professional communications
- Personal devices must be switched to silent during lessons
- Emergency contact should be via school office
- Professional boundaries must be maintained

7.3 Digital Images and Video

- Parental consent required for all student images
- Students not identified by name in online publications
- No personal information embedded in image files
- Professional use only for school-related purposes
- Secure storage and appropriate sharing protocols

---

8. INCIDENT MANAGEMENT AND REPORTING

8.1 Types of Incidents

We recognise four main categories of online risk as defined by KCSIE 2025:

Content Risks:

- Exposure to illegal content (as defined by the Online Safety Act 2023)
- Age-inappropriate material including pornography and violence
- Content promoting self-harm, suicide, or eating disorders
- Misinformation, disinformation, fake news, and conspiracy theories
- Extremist or terrorist content
- Content encouraging dangerous behaviours or substance abuse

Contact Risks:

- Grooming and child sexual exploitation
- Online predatory behaviour
- Unwanted contact from adults or strangers
- Cyberbullying, harassment, and abuse
- Identity theft and impersonation

Conduct Risks:

- Inappropriate sharing of personal information
- Sexting and sharing of intimate images
- Online reputation damage and digital footprint concerns
- Cyberbullying perpetrated by the individual
- Copyright infringement and illegal downloading
- Engaging in illegal activities online

Commerce Risks:

- Online gambling and betting
- Inappropriate commercial exploitation
- Financial scams and fraud
- In-app purchases and financial manipulation

8.2 Reporting Procedures

Students should:

- Tell a trusted adult immediately
- Not delete evidence of incidents
- Not respond to inappropriate communications
- Seek support from school staff or counsellors

Staff should:

- Report incidents immediately to E-Safety Coordinator
- Document incidents thoroughly
- Preserve evidence where appropriate
- Follow safeguarding procedures for serious concerns

8.3 Response Procedures

Our response includes:

- Immediate risk assessment and safeguarding measures
- Compliance with Online Safety Act reporting requirements to Ofcom where applicable
- Safeguarding referrals to Children's Services and Police as required
- Data breach notifications to ICO within 72 hours where personal data is involved
- Support for affected students, families, and staff
- Evidence preservation following legal requirements
- Investigation and root cause analysis
- Policy and practice review and improvement
- Multi-agency liaison including local authority, police, and regulatory bodies

8.4 Regulatory Reporting

Required reporting under current legislation:

- **Online Safety Act 2023:** Serious online safety incidents to Ofcom
- **KCSIE 2025:** Safeguarding incidents to local authority and Children's Services
- **UK GDPR/Data Protection Act:** Personal data breaches to ICO
- **Education Act:** Serious incidents to Department for Education
- **Local Authority:** All significant e-safety incidents via established procedures

8.4 Sanctions

Depending on the severity of incidents, responses may include:

- Additional e-safety education
- Restricted technology access
- Formal disciplinary procedures
- Involvement of parents/carers
- External agency referrals
- Police involvement for illegal activities

---

9. MONITORING AND REVIEW

9.1 Regular Monitoring

- **Monthly:** Review of incident logs and filtering effectiveness
- **Quarterly:** Policy effectiveness assessment and staff training needs review
- **Bi-annually:** Technical security assessment and penetration testing
- **Annually:** Full policy review, stakeholder feedback collection, and compliance audit
- **Ongoing:** Monitoring of Online Safety Act implementation and regulatory changes

9.2 Compliance Monitoring

Regulatory compliance tracking:

- **Online Safety Act 2023:** Platform duty compliance and Ofcom guidance updates
- **KCSIE 2025:** Annual self-assessment of filtering and monitoring arrangements

- **UK GDPR:** Data audit cycle and privacy impact assessments
- **Data (Use and Access) Act 2025:** New provisions implementation
- **Local Authority:** Regular liaison and reporting requirements

9.2 Policy Review

This policy will be reviewed annually or following significant incidents, ensuring it remains:

- Current with technological developments
- Compliant with legal requirements
- Effective in protecting our community
- Supportive of educational objectives

9.3 Reporting and Governance

- Regular reports to Senior Leadership Team
- Termly updates to governing body
- Annual e-safety report to stakeholders
- Liaison with local authority and external partners

---

10. SUPPORT AND RESOURCES

10.1 Internal Support

- E-Safety Coordinator: Available for all e-safety concerns
- Designated Safeguarding Lead: For safeguarding-related incidents
- School Counsellors: For students affected by online incidents
- IT Support Team: For technical issues and guidance

10.2 External Resources

For Students:

- Childline: 0800 1111 / www.childline.org.uk
- CEOP Report Abuse: www.ceop.police.uk/safety-centre
- Internet Watch Foundation: www.iwf.org.uk
- Young Minds: 0808 802 5544 / www.youngminds.org.uk
- Report Harmful Content: www.reportharmfulcontent.com

For Parents:

- Internet Matters: www.internetmatters.org
- UK Safer Internet Centre: www.saferinternet.org.uk
- National Online Safety: www.nationalonlinesafety.com
- Parentline Plus: 0808 800 2222
- Family Lives: 0808 800 2222

For Staff:

- Professional Online Safety Helpline: 0344 381 4772
- NSPCC: 0808 800 5000
- Education Support: 08000 562 561
- ICO: 0303 123 1113 / ico.org.uk

Regulatory Bodies:

- Ofcom (Online Safety): www.ofcom.org.uk/online-safety
- Information Commissioner's Office: ico.org.uk
- Department for Education: 0370 000 2288

---

11. POLICY COMMUNICATION

This policy is communicated through:

- School website and learning platform
- Staff induction programmes
- Student assemblies and lessons

- Parent information sessions
- Governor training sessions
- Regular newsletter updates

Policy Approved by: Allan Lacey, Headteacher
Date: September 2025
Review Date: September 2026

This policy reflects our commitment to providing a safe, supportive digital environment for all members of our school community, with particular attention to the needs of students with autism spectrum conditions. The policy is fully compliant with the Online Safety Act 2023, KCSIE 2025, UK GDPR, and all current statutory requirements.

Document Control:

- Version: 2025.1
- Approved: Allan Lacey (Headteacher)
- Implementation: September 2025
- Review Cycle: Annual (or following significant incidents/regulatory changes)

Key Legislative Compliance:

- ✓ Online Safety Act 2023 (Child Safety Codes)
- ✓ Keeping Children Safe in Education 2025
- ✓ UK GDPR and Data Protection Act 2018
- ✓ Data (Use and Access) Act 2025
- ✓ DfE Filtering and Monitoring Standards 2024