# Bryn St. Peter's C.E. Primary School


# Online Safety Policy

Our School Vision

# Together with God Building our Future

Guided by Christian values, with Jesus as our cornerstone, we set firm foundations for a life of flourishing, offering opportunities for all to develop in body, mind and spirit.

*And in him you too are being built together to become a dwelling in which God lives by his Spirit.*

Ephesians 2:22

We are committed to educating the whole person for life in all its fullness guided by Christian values.
We deeply value creativity and joy in learning that allows everyone to achieve and flourish.
We want everyone to feel included, accepted, loved and positively understand their value and potential in our community.

**Introduction**

At Bryn St Peter's, we recognise that technology plays an increasingly important role in children's lives both inside and outside school. Online safety is a fundamental aspect of safeguarding and is embedded throughout our curriculum, policies and daily practice.

We are committed to ensuring that all pupils learn how to use technology safely, responsibly and respectfully. Through education, monitoring, filtering systems, staff training and strong partnerships with parents and carers, we aim to develop confident and responsible digital citizens.

The purpose of this policy is to guide the teaching, learning and leadership of Online Safety at Bryn St Peter's, ensuring a consistent, high-quality approach from Reception to Year 6.

**2. Aims and Objectives**

**Aims**

Our Online Safety curriculum aims to ensure that all pupils:

- Become safe, responsible and respectful users of technology.
- Understand how to keep themselves and others safe online.
- Recognise and manage online risks.
- Know how and when to seek help from trusted adults.
- Develop positive digital citizenship skills.

- Are prepared for the opportunities and challenges of an increasingly digital world.
- Develop an understanding of basic cyber security principles, including creating strong passwords, protecting personal information and recognising potential online threats.

**Objectives**

Pupils will be taught to:

- Keep personal information private and secure.
- Understand safe online communication
- Recognise cyberbullying and know how to respond.
- Evaluate online information critically.
- Understand the importance of privacy and security settings.
- Demonstrate respectful online behaviour.
- Identify trusted adults and reporting systems.
- Recognise that not everything online is accurate or trustworthy.

**3. Curriculum Intent**

Our intent is to provide a progressive Online Safety curriculum that equips pupils with the knowledge, skills and understanding needed to navigate the digital world safely and confidently.

Online Safety at Bryn St Peter's is designed to:

- Provide clear progression from EYFS through to Year 6.
- Support the safeguarding of all pupils.
- Meet the expectations of the National Curriculum and Keeping Children Safe in Education.
- Promote the values of responsibility, respect, resilience and kindness.
- Develop pupils' understanding of online risks and how to respond appropriately.
- Foster positive digital citizenship and healthy online behaviours.
- Utilise high-quality resources, primarily through Purple Mash.
- Develop pupils' understanding of cyber security and how to protect themselves, their devices and their information online
- Cyber security is taught progressively throughout the school to help pupils understand how to protect themselves, their personal information and the technology they use in an increasingly connected world.

**4. Implementation**

**Teaching Across the School**

- Purple Mash Online Safety resources are used as the core scheme from Reception to Year 6.

- EYFS pupils explore technology safely through play-based learning and adult-led discussion.
- KS1 pupils learn about personal information, trusted adults and safe online behaviours.
- KS2 pupils develop a deeper understanding of online communication, privacy, cyberbullying, misinformation and digital footprints.
- Online Safety is taught through Computing lessons, PSHE, assemblies and safeguarding activities.
- The school participates annually in Safer Internet Day.
- Where appropriate, pupils are introduced to emerging technologies, including artificial intelligence, and taught how to use technology critically, safely and responsibly.
- Pupils are taught age-appropriate cyber security skills, including password security, protecting personal information, recognising phishing and scams, understanding privacy settings and keeping devices secure

**Teaching and Learning Approaches**

- Lessons include modelling, discussion and scenario-based learning.
- Pupils are encouraged to think critically about online situations.
- Real-life examples are used where appropriate.
- Online Safety themes are revisited regularly to support retention and progression.
- Pupils are taught how to report concerns and seek support.

**Cross-Curricular Links**

Online Safety is integrated across the curriculum, particularly within:

- Computing
- PSHE
- Religious Education
- Safeguarding education
- Anti-bullying work

**Resources and Technology**

The school uses:

- Purple Mash Online Safety resources.
- Securus filtering and monitoring systems.
- CPOMS safeguarding recording system.
- Laptops, iPads and Kindles.
- Interactive screens.
- Assemblies and awareness materials.
- Monthly Online Safety newsletters.
- Filtering and monitoring systems are reviewed regularly to ensure they remain effective and appropriate.

**Inclusion and Differentiation**

Adaptive teaching strategies include:

- Scaffolded activities and visual supports.
- Simplified language where appropriate.
- Small-group discussions and adult support.
- Alternative recording methods.
- Additional support for SEND and EAL pupils.
- Opportunities for deeper discussion and leadership for pupils working at greater depth.

## 5. Impact

**Measuring Effectiveness**

Impact is measured through:

- Pupil discussions and pupil voice activities
- Purple Mash Online Safety activities.
- Formative assessment during lessons.
- Safeguarding records and trends.
- Monitoring of online incidents.
- Staff confidence and training records.
- Feedback from parents and carers.

**Expected Pupil Outcomes**

By the end of KS2, pupils will:

- Understand how to stay safe online
- Demonstrate responsible digital citizenship.
- Recognise online risks and know how to respond.
- Understand the importance of protecting personal information.
- Communicate respectfully online
- Know how to seek help and report concerns.
- Understand the importance of strong passwords and secure accounts.
- Recognise common online risks such as scams, phishing and unsafe downloads.
- Know how to protect personal information online.
- Understand basic cyber security practices that help keep devices and data secure.

**Celebrating Success**

- Safer Internet Day activities.
- Assemblies and class displays.
- Online Safety competitions and projects. Celebration of positive digital citizenship.
- Sharing key learning through newsletters and school communications.

## 6. Planning and Progression

### Planning Expectations

- Long-term plans outline Online Safety coverage across year groups.
- Medium-term plans follow Purple Mash Online Safety units and align with school progression documents.
- Short-term plans include learning objectives, vocabulary, progression and adaptive teaching strategies.

### Progression of Skills

- Skills progress through Reception → KS1 → Lower KS2 → Upper KS2.
- Online Safety knowledge is revisited and developed throughout each year group.
- Purple Mash provides a clear progression framework to ensure age-appropriate coverage and consistency.

## 7. Assessment and Monitoring

### Assessment

- Formative assessment through observation, discussion and questioning.
- Purple Mash activities provide opportunities to assess understanding.
- Teachers assess pupils' ability to apply Online Safety knowledge in different contexts.

### Use of Assessment

Teachers use assessment to:

- Identify misconceptions.
- Plan future learning.
- Provide targeted support.
- Address emerging online safety concerns.

### Monitoring

The Computing Subject Leader, DSL and Senior Leadership Team monitor:

- Curriculum coverage.
- Teaching and learning.
- Pupil understanding.
- Safeguarding incidents linked to technology.
- Filtering and monitoring reports.
- Staff training needs.
- All online safety concerns are recorded and managed through CPOMS in line with safeguarding procedures.

## 8. Role of the Subject Leader

The Computing/Online Safety Lead is responsible for:

- Leading and developing Online Safety provision.
- Monitoring the effectiveness of the Online Safety curriculum.
- Supporting staff with planning and teaching.
- Keeping up to date with current guidance and emerging risks.
- Delivering or facilitating staff training.
- Working alongside the DSL to ensure effective safeguarding procedures.
- Monitoring filtering and monitoring systems.
- Reporting developments and priorities to senior leaders and governors.

**9. Resources**

Key resources include:

- Purple Mash Online Safety Scheme.
- Securus filtering and monitoring.
- CPOMS safeguarding system.
- Laptops, iPads and Kindles.
- Online Safety newsletters.
- National Online Safety resources.
- Assembly materials and awareness campaigns.

Resources are reviewed annually following an audit by the Subject Leader.

**10. Inclusion and Equal Opportunities**

The Online Safety curriculum promotes equality by:

- Ensuring all pupils can access learning through adaptive teaching.
- Providing additional support for SEND and EAL pupils.
- Promoting respectful online behaviour for all.
- Teaching pupils to value diversity and challenge discrimination online.
- Encouraging positive and inclusive digital citizenship.

**11. Health and Safety**

- Pupils follow clear rules for safe and responsible use of technology.
- Online risks are minimised through filtering and monitoring provided by Securus.
- Staff receive regular safeguarding and online safety training.
- Concerns are recorded through CPOMS and managed in line with safeguarding procedures.
- Pupils are taught how to report concerns to trusted adults.
- Digital wellbeing and healthy technology use are promoted throughout the curriculum.

- Any online safety concern that presents a safeguarding risk will be managed in accordance with the school's Safeguarding and Child Protection Policy and referred to the Designated Safeguarding Lead without delay.

**12. Parental and Community Links**

- Parents receive monthly Online Safety newsletters.
- Online Safety guidance is shared through school communication systems.
- Families are informed of current trends and risks affecting children online.
- Parents are encouraged to support safe technology use at home.
- Safer Internet Day resources and activities are shared with families where appropriate.

**13. Review and Evaluation**

- This policy will be reviewed annually.
- The Computing/Online Safety Lead, DSL and Headteacher are responsible for evaluating the effectiveness of Online Safety provision.
- Adjustments will be made based on safeguarding trends, monitoring outcomes, staff feedback and developments in technology and guidance.
- Governors receive updates regarding online safety provision, filtering and monitoring arrangements, staff training and safeguarding trends as part of their responsibility for ensuring effective safeguarding arrangements.

**14. Linked Policies and Documents**

This policy should be read alongside:

- Safeguarding and Child Protection Policy
- Computing Policy
- Behaviour Policy
- Staff Code of Conduct
- Social Media Policy
- Data Protection Policy
- PSHE Policy
- SEND Policy
- Anti-Bullying Policy
- Remote Learning Policy
- Acceptable Use Agreements
- Keeping Children Safe in Education (KCSIE)