BRYN DERI PRIMARY SCHOOL

Online Safety Policy

2026-2027

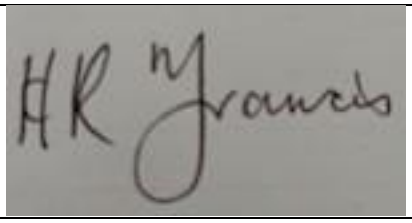
Our commitment

At Bryn Deri Primary School, we want every user to be safe, confident and supported when using technology — whether learning in school, at home, or in the wider community. Online safety is part of safeguarding and wellbeing. It is not simply an IT issue: it is about people, relationships, behaviour, learning and protection.

School	Bryn Deri Primary School
Designated Safeguarding Persons	Mr Ian Russell • Miss Patricia Evans • Mr Alex Davies

Arrangements for reviewing the policy

- The implementation of this policy is the responsibility of all stakeholders
- Staff and Governors will review the policy when there are major updates or every year

Date Approved by FGB	14-10-26
Signed on behalf of FGB	
Name (Chair of Governors)	Mrs H. Francis
Date	14-10-26
Date of next review	October 2027

Adapted and professionally formatted from the supplied SWGfL Online Safety Policy Statement scaffold.

Contents

1. Purpose and commitment
2. Scope
3. Policy principles and outcomes
4. Leadership, roles and accountability
5. Education, curriculum and staff development
6. Acceptable and responsible use
7. Reporting, recording and responding to concerns
8. Technology, filtering and monitoring
9. Cyber security and data protection
10. Digital content, communication and consent
11. Partnership with families and agencies
12. Impact review and continuous improvement
13. How to raise a concern or get help
14. Review and approval

Appendix 1 – Roles and responsibilities
Appendix 2 – Acceptable use expectations
Appendix 3 – Reporting and response pathway
Appendix 4 – Online safety education framework
Appendix 5 – Technical safeguards and cyber resilience
Appendix 6 – Data protection and digital content
Appendix 7 – Family guidance and communication
Appendix 8 – Impact review checklist

Important note about the supplied scaffold

The uploaded September 2026 scaffold contains the four core outcome areas — Leadership and policy, Education, Technology and Impact — but does not contain a separate appendix section. The appendices in this policy have therefore been added to operationalise and organise the commitments in the supplied scaffold; they do not replace the school's existing safeguarding, behaviour, acceptable-use, data-protection or technical procedures.

1. Purpose and commitment

This policy sets out how Bryn Deri Primary School will promote safe, respectful and positive use of technology. Online safety is embedded within safeguarding and wellbeing and applies to pupils, staff, governors, volunteers, families and other users of school technology or school-managed digital services.

- We want every user to be safe, confident and supported when using technology.
- We recognise that online safety is about people, relationships, behaviour, learning and protection, not only IT.
- We will provide clear expectations, appropriate education, proportionate technical safeguards and regular review.
- We will respond to concerns consistently, record appropriately and use learning from incidents to improve practice.

2. Scope

This policy applies to online activity connected with school, including use of school devices, accounts, networks, digital learning platforms, communications and online services. It also recognises that online experiences outside school can affect pupils, staff and the wider school community.

- Pupils using technology for learning or school-related activities.
- All staff, governors, volunteers and other adults working with or supporting the school.
- Parents and carers where school systems, communications or online-safety guidance are involved.
- School-managed devices, networks, accounts, platforms and digital content.
- Online concerns that may affect safeguarding or wellbeing, even where the activity began outside school.

3. Policy principles and outcomes

Our online safety strategy is built around four outcomes-focused areas that strengthen day-to-day practice:

Area	Intended outcome
Leadership and policy	Clear expectations, defined responsibilities, consistent reporting and accountability.
Education	Knowledge, skills, resilience and positive online behaviour for learners and informed adults.
Technology	Proportionate protection that supports safe teaching and learning.
Impact review	Regular evidence-based review of what is working and what should improve.

4. Leadership, roles and accountability

Strong leadership makes online safety part of how we work at Bryn Deri Primary School rather than a one-off initiative. Responsibilities are defined so safeguarding decisions, education and technical safeguards work together.

Designated Safeguarding Persons

- Mr Ian Russell
- Miss Patricia Evans
- Mr Alex Davies

The Designated Safeguarding Persons provide a clear route for parents/carers and staff to raise online-safety concerns and ensure that safeguarding concerns are dealt with through the school's established safeguarding procedures.

Whole-school accountability

- Senior leaders provide direction, oversight and accountability for online safety.
- The safeguarding team supports the identification, escalation and response to online-safety concerns.
- Staff model safe, respectful and responsible digital practice.
- Governors provide challenge and support and consider policy, training, curriculum, filtering/monitoring and cyber security.
- Technical staff or providers support secure systems, appropriate filtering, monitoring and cyber resilience.
- Where appropriate, learners and families contribute to review so that online safety reflects real experiences and emerging risks.

5. Education, curriculum and staff development

Online safety education is progressive, inclusive and revisited regularly. Teaching aims to build knowledge, skills, attitudes and resilience so that learners can enjoy the benefits of technology while managing risk.

- Online safety is taught as part of planned learning and reinforced through day-to-day school life.
- Learner voice may be used to identify concerns and shape relevant teaching.
- Pupils are encouraged to make safer choices, develop healthy online behaviour and know how to seek help.
- All staff receive induction and ongoing updates so they can identify concerns, respond appropriately and model safe practice.
- Key roles receive enhanced training where needed to support informed safeguarding decisions.
- Governors are supported to understand their responsibilities and ask appropriate questions about online safety.

6. Acceptable and responsible use

We set simple, age-appropriate expectations for learners and clear professional expectations for adults. Safe and respectful use applies to school devices, accounts, networks, platforms and communications.

- Technology is used for appropriate educational, professional or school-related purposes.
- Users behave respectfully and consider the impact of their words, images and actions on others.
- Users protect passwords, personal information and access to school systems.
- Concerns, unsafe content, suspicious messages or inappropriate behaviour are reported promptly.
- Personal devices are used only in line with school expectations and safeguarding requirements.
- Digital content is used, shared and published responsibly, with appropriate safeguarding and consent considerations.

7. Reporting, recording and responding to concerns

We promote a culture where people feel able to speak up. Concerns are responded to consistently, recorded appropriately, acted on promptly and used to identify patterns and emerging risks.

- Pupils can speak to a trusted adult, class teacher, teaching assistant or member of the safeguarding team.
- Parents and carers can contact Mr Ian Russell, Miss Patricia Evans or Mr Alex Davies.
- Staff follow safeguarding procedures and record concerns promptly.
- Concerns are escalated through established safeguarding routes where required.
- The school considers the welfare of the child or adult affected and the need for proportionate intervention.
- Patterns, repeated concerns and emerging risks are considered during review and improvement activity.

8. Technology, filtering and monitoring

Technology should protect users while enabling effective teaching and learning. The school uses proportionate technical controls to reduce exposure to harmful or illegal content and to support timely safeguarding intervention.

- Filtering is used to reduce the risk of access to harmful and illegal content.
- Filtering is reviewed to ensure it remains fit for purpose.
- Monitoring supports early identification of concerns and timely intervention, with appropriate governance and data-protection considerations.
- Networks, devices and accounts are protected through appropriate security measures.
- The school prepares for threats such as phishing and ransomware to reduce disruption and protect users.
- Technical incidents and safeguarding concerns are connected through clear reporting and escalation routes.

9. Cyber security and data protection

We handle personal and sensitive information carefully and lawfully, with clear processes and accountability. Cyber resilience is part of online safety because secure systems help protect people as well as learning.

- Users are expected to protect accounts, passwords and devices.
- Suspicious emails, links, attachments or requests for information are reported.
- The school takes reasonable steps to protect networks, devices and digital services.
- Personal and sensitive information is handled with appropriate care.
- Digital information is shared only where there is a legitimate and appropriate reason to do so.
- The school learns from incidents and improves its protective measures where required.

10. Digital content, communication and consent

The school manages digital content consistently and communicates responsibly through its public and internal channels.

- Images, videos and other digital content involving pupils are handled in line with school safeguarding and consent arrangements.
- Staff and pupils communicate respectfully through school-managed channels.
- Public communications are considered carefully before publication.
- Users avoid sharing personal or sensitive information unnecessarily.

- Concerns about digital content are reported promptly rather than shared further.

11. Partnership with families and agencies

Online safety is strongest when children experience consistent expectations between school and home. The school will communicate practical guidance to families and work with relevant partners where this supports safer communities.

- Families receive practical, age-appropriate online-safety guidance where appropriate.
- The school encourages parents/carers to raise concerns early.
- Relevant external agencies or partners may be involved when this is appropriate to safeguarding or technical risk.
- Where useful, effective practice and learning may be shared beyond school to support safer communities.

12. Impact review and continuous improvement

We regularly review how well our policy and practice are working, what evidence tells us and what should improve next. This keeps our approach current, targeted and effective.

- Review incidents, concerns and emerging themes.
- Consider staff, pupil, governor and family feedback where appropriate.
- Review the effectiveness of education and training.
- Review filtering, monitoring and technical safeguards.
- Identify actions, owners and timescales for improvement.
- Record significant learning and use it to inform future practice.

13. How to raise a concern or get help

> **If something online worries you, we want to know.**
>
> Speaking up early can help the school provide support and take appropriate safeguarding action.

Learners

- Talk to a trusted adult, your class teacher or teaching assistant, or a member of the safeguarding team.

Parents and carers

- Contact Mr Ian Russell, Miss Patricia Evans or Mr Alex Davies.

Staff

- Follow safeguarding procedures and record concerns promptly.

14. Review and approval

Policy owner	Bryn Deri Primary School
Approved	September 2026

Review date	September 2027, or earlier if legislation, guidance, technology, school arrangements or safeguarding learning require it
Related school procedures	Safeguarding procedures; acceptable-use expectations; behaviour procedures; data protection arrangements; technical/security procedures

Appendices

The supplied scaffold did not contain a separate appendix section. The following appendices have been added to make the policy practical and easy to implement while retaining the four outcome areas and commitments in the supplied document.

Appendix 1 – Roles and responsibilities

Role	Who	Key responsibility
Designated Safeguarding Persons	Mr Ian Russell; Miss Patricia Evans; Mr Alex Davies	Provide a clear safeguarding route for online-safety concerns and ensure concerns are managed through established safeguarding procedures.
Senior leadership	Mr Ian Russell; Miss Patricia Evans; Mr Alex Davies	Provide strategic oversight, ensure expectations are clear, support training and review impact.
All staff	All school staff and relevant adults	Model safe digital behaviour, follow acceptable-use expectations, identify concerns and report/record them promptly.
Governors	Governing body	Provide challenge and support and consider policy, training, curriculum, filtering/monitoring and cyber security.
Technical support	School technical staff/providers	Support secure systems, appropriate filtering and monitoring, device/account security and cyber resilience.
Learners	All pupils	Use technology respectfully, follow age-appropriate expectations, protect personal information and tell a trusted adult when something causes concern.
Parents/carers	Families	Support safe and respectful use at home, engage with school guidance and raise concerns early.

Appendix 2 – Acceptable use expectations

For learners

- Use technology for learning and other purposes agreed by the school.
- Be kind, respectful and responsible in messages, comments, images, games and other online activity.
- Keep passwords and personal information private.
- Do not deliberately search for, access, create or share harmful or inappropriate material.
- Tell a trusted adult if something online feels unsafe, upsetting, confusing or inappropriate.
- Do not use another person's account or pretend to be another person.
- Use school devices and networks carefully and report damage, loss or suspicious activity.

For staff and other adults

- Use school systems and digital services responsibly and professionally.
- Protect passwords, devices and access to school systems.
- Maintain appropriate professional boundaries in digital communication.
- Do not share personal or sensitive information unless there is an appropriate reason and route.
- Use images, video and other digital content in line with safeguarding and consent arrangements.
- Report online-safety, safeguarding or cyber-security concerns promptly.
- Follow school procedures when using personal devices in connection with school activity.

Appendix 3 – Reporting and response pathway

1. Speak up: A pupil, parent/carer or member of staff reports an online-safety concern.

2. Listen and reassure: The concern is taken seriously and the person is supported.

3. Record: Relevant information is recorded promptly and accurately in line with school procedures.

4. Safeguarding decision: The concern is considered through the school's safeguarding arrangements, including escalation where required.

5. Appropriate action: The school takes proportionate action to support the individual, manage risk and address the issue.

6. Review: Patterns, learning and emerging risks are considered so that practice can improve.

> **Do not investigate alone**
>
> Where an online concern may involve safeguarding risk, staff should follow the school's safeguarding procedures and seek support from the Designated Safeguarding Persons rather than attempting to resolve the matter informally.

Appendix 4 – Online safety education framework

Area	School approach
Knowledge	Understand common online risks, privacy, personal information, online communication and how digital content can spread.

Area	School approach
Skills	Develop practical skills for safer searching, account security, reporting, blocking and seeking help.
Attitudes	Promote respect, empathy, responsibility and thoughtful decision-making.
Resilience	Help learners manage setbacks, upsetting content, peer pressure and changing online experiences.
Help-seeking	Ensure learners know trusted adults and feel confident to report concerns.
Learner voice	Use pupil experiences and feedback, where appropriate, to keep teaching relevant to real-life online challenges.

Appendix 5 – Technical safeguards and cyber resilience

- Maintain appropriate filtering to reduce access to harmful and illegal content.
- Review filtering so that it remains fit for purpose and supports learning.
- Use safeguarding-led monitoring to help identify concerns early, with appropriate governance and data-protection controls.
- Protect networks, devices and accounts through appropriate security measures.
- Promote awareness of phishing, suspicious links, malicious attachments and other common cyber threats.
- Prepare for incidents such as ransomware or service disruption so that learning can continue and recovery is as effective as possible.
- Manage devices consistently, including expectations around personal devices where relevant.

Balance protection and learning

Technical controls should be proportionate: they should reduce avoidable risk while enabling effective teaching, learning and legitimate educational use of technology.

Appendix 6 – Data protection and digital content

- Handle personal and sensitive information carefully and lawfully.
- Share information only through appropriate channels and for appropriate purposes.
- Protect accounts and devices that provide access to personal information.
- Use safeguarding and consent arrangements when creating, storing or sharing digital content involving pupils.
- Check public communications before publication and avoid unnecessary disclosure of personal information.
- Report suspected loss, inappropriate disclosure, account compromise or other data/cyber concerns promptly.

Appendix 7 – Family guidance and communication

The school will encourage families to take an active role in online safety. Guidance should be practical, age-appropriate and consistent with the expectations children experience in school.

- Talk regularly with children about what they do online and who they communicate with.
- Encourage children to speak to a trusted adult when something online worries them.
- Support children to protect passwords and personal information.
- Use appropriate parental controls and device settings where suitable for the child's age and needs.
- Encourage respectful behaviour online and explain that online actions can affect other people.
- Contact the school early if an online issue is affecting a child's wellbeing, relationships or ability to learn.

School contacts

For online-safety concerns, parents/carers can contact Mr Ian Russell, Miss Patricia Evans or Mr Alex Davies.

Appendix 8 – Impact review checklist

☐ Have online-safety roles and responsibilities remained clear?

☐ Have staff received appropriate induction and ongoing updates?

☐ Is online-safety education progressive, inclusive and relevant?

☐ Have pupil and family concerns or feedback identified any emerging themes?

☐ Are reporting and recording arrangements working consistently?

☐ Has filtering been reviewed and found fit for purpose?

☐ Has monitoring been reviewed in line with safeguarding and data-protection requirements?

☐ Are devices, accounts and networks appropriately protected?

☐ Have there been any cyber-security incidents or near misses that require learning?

☐ Are digital content and consent arrangements understood and followed?

☐ What actions should be taken next, who owns them and when should they be reviewed?

Source and attribution

This policy has been professionally reformatted and expanded from the document supplied for editing: “Online Safety Policy Statement – September 2026”, © SWGfL 2026.

The supplied document states that SWGfL school online safety policy templates may be used free of charge by schools and other educational institutions, with acknowledgement of use. It also notes that the template reflects information available at the date of publication in August 2026 and recommends suitable legal/professional advice where difficulties arise.

School-specific note: The additional appendices in this edited version organise the commitments in the supplied scaffold into practical school-facing sections. They should be read alongside the school’s own safeguarding, behaviour, acceptable-use, data-protection and technical procedures.