Barkisland CE (VA) Primary School

ESafety and AI Policy

Introduction
At Barkisland Primary School, we are committed to preparing our pupils for life in an increasingly digital world. Technology is embedded in education, communication, and society, offering vast opportunities for learning, creativity, and collaboration. However, it also presents risks such as cyberbullying, exposure to harmful content, misuse of personal data, and the ethical implications of Artificial Intelligence (AI).

This policy outlines our approach to ensuring all members of our school community can engage with digital technologies confidently, safely, and responsibly. It reflects our duty to safeguard pupils in both physical and online environments and supports our wider aim of promoting digital resilience and ethical awareness.

Becky Schofield, Headteacher, holds **ultimate responsibility** for the e-Safety of the school community.

Sarah Wilde, as the school's designated **eSafety Lead**, has day-to-day responsibility for eSafety implementation, staff support, and system monitoring.

1. Frameworks and Statutory Guidance
This policy aligns with and is informed by the following key national documents and frameworks that set standards and best practices for online safety and the ethical use of technology and AI in education:

- **Keeping Children Safe in Education (KCSiE) 2025**
  This statutory guidance requires schools to safeguard children from online harm, including risks such as cyberbullying, inappropriate content, and grooming. It mandates that staff are trained in online safety and that pupils receive age-appropriate education on digital risks and responsibilities. The guidance places a strong emphasis on embedding online safety within wider safeguarding arrangements.

- **UK Council for Internet Safety (UKCIS): Education for a Connected World**
  This framework provides comprehensive guidance on digital literacy development across eight key strands, including online reputation, self-image, online relationships, privacy, health, and wellbeing. It offers detailed progression statements to help schools deliver consistent, age-appropriate teaching that empowers children to use technology safely and positively.

- **Department for Education (DfE): Teaching Online Safety in Schools**
  This guidance advocates for online safety education to be embedded throughout the curriculum and tailored to pupils' developmental stages. It encourages schools to build

resilience, teach critical thinking skills, and cover emerging risks such as those posed by AI technologies. The document supports a whole-school approach involving staff, pupils, and parents.

- **DfE Filtering and Monitoring Standards (2023)**
  This updated standard sets out the expectations for schools to implement robust filtering and monitoring systems that prevent access to harmful and inappropriate online content. It requires schools to regularly review the effectiveness of these systems, ensure transparency in their operation, and have clear roles for staff overseeing filtering and monitoring.
- **Information Commissioner's Office (ICO) Guidance on Children and the GDPR and AI in Education**
  This guidance clarifies how schools must comply with data protection laws when using digital and AI technologies, particularly regarding children's personal data. It highlights lawful processing, transparency, safeguarding against profiling or bias, and the importance of Data Protection Impact Assessments (DPIAs) when implementing new AI tools or data-driven systems in schools.

2. Purpose
This policy outlines our approach to ensuring the safety, wellbeing, and digital literacy of pupils, staff, and the wider school community. It aims to protect users from online risks, foster responsible use of digital technologies, and guide the safe integration of AI in education.

3. Scope
This policy applies to all pupils, staff, volunteers, governors, and visitors who access or use school technology, including AI tools. It covers all digital devices, networks, internet services, and platforms used within or associated with the school.

4. Vision and Values
Our vision is to equip pupils with the knowledge and skills to use technology safely, respectfully, and responsibly. Our approach is underpinned by our core values:

- **Believe** – empowering pupils to believe in their ability to navigate the digital world safely and with confidence.
- **Aspire** – encouraging high standards of digital literacy, resilience, and ambition in how technology is used.
- **Respect** – fostering a respectful digital culture where all interactions online reflect our expectations of kindness and care.
- **Koinonia** – promoting community and unity, online and offline, through shared responsibility and support.

- **Inclusive** – ensuring all pupils, regardless of background or need, access safe, supportive digital experiences.
- **Success** – equipping children with the skills they need to succeed in a connected, digital society.
- **Love** – caring for others online through empathy, compassion, and encouragement.
- **Nurture** – building safe learning environments where children grow in confidence, supported to make informed and ethical choices online.
- **Dream** – inspiring pupils to use technology creatively and imaginatively, exploring new possibilities and shaping a positive digital future.

5. Roles and Responsibilities

Governing Body

- Ensure the policy is reviewed annually and complies with statutory guidance.
- Support and monitor the school's eSafety and AI practices.
- Ensure appropriate resources and funding are available.

Senior Leadership Team (SLT)

- **Becky Schofield (Headteacher)** holds **ultimate responsibility** for eSafety.
- **Sarah Wilde (eSafety Lead)** manages day-to-day eSafety operations, monitors incidents via CPOMS and filtering alerts, leads training and sign-posts staff to any relevant training.
- Ensure technical support is adequate to maintain a secure ICT environment.
- Liaise with governors regarding eSafety and data protection.
- Promote an inclusive, respectful eSafety culture reflecting school values.
- Ensure all users agree to the Acceptable Use Policy (AUP) and eSafety is part of new staff induction.
- Regularly review eSafety incident logs on CPOMS and ensure proper follow-up.

Designated Safeguarding Lead (DSL)

- Lead on safeguarding and eSafety incident response.
- Support pupils and staff in cases of online harm or AI misuse.

All Staff

- Read and actively promote eSafety policies and guidance.
- Sign and adhere to staff Acceptable Use Policy.
- Take responsibility for securing sensitive data and ICT resources.
- Maintain awareness of eSafety issues, legislation, and guidance.

- Model professional and safe conduct in all personal technology use.
- Communicate digitally only via school-approved channels (e.g., no personal emails or social media contact with pupils/parents).
- Embed eSafety teaching in lessons and supervise pupils' digital use carefully.
- Report all eSafety incidents promptly and log them on CPOMS under the eSafety category.
- Respect others' rights, feelings, and intellectual property in all technology use.

Pupils

- Follow the pupil Acceptable Use Policy (AUP), which is included at the end of this policy document.
- All pupils will sign the AUP, and copies will be displayed prominently in every classroom to reinforce safe and responsible technology use.
- Take responsibility for their own and others' safe technology use, including personal devices outside school.
- Respect others' feelings, rights, and values in online behaviour.
- Know how and when to report concerns or harmful content.
- Discuss eSafety openly with family and friends.
- Follow school policies on mobile phones, cyberbullying, and digital content.

Parents and Carers

- Support and promote the school's eSafety approach at home.
- Read, understand, and reinforce the pupil AUP.
- Discuss safe technology use with their children regularly.
- Sign agreements regarding the use of pupil images and responsible social media use:

"We will support the school's approach to online safety and will not deliberately post comments or upload any images, sounds, or text that could upset or offend any member of the school community or bring the school into disrepute."

6. e-Safety Education

Pupils receive ongoing, age-appropriate education through Computing and PSHE, covering:

- Responsible online behaviour, kindness, and anti-cyberbullying.
- Protection of personal data and understanding digital footprints.
- Critical evaluation of online content including AI-generated material.
- Reporting online harms and developing upstander behaviours.
- Digital rights, responsibilities, and respecting others online.

7. Use of Artificial Intelligence (AI)

Artificial Intelligence (AI) technologies are rapidly evolving and increasingly impacting education, offering new tools for learning, assessment, and administration. Barkisland Primary School embraces AI cautiously and responsibly, ensuring its safe and ethical integration into the educational environment.

Educational Use of AI

AI may be used to:

- Support **personalised learning** through adaptive platforms that respond to pupils' individual needs and progress.
- Assist staff with **lesson planning**, resource creation, and administrative tasks, improving efficiency.
- Enhance **creative learning**, enabling pupils to explore digital art, storytelling, music, and coding with AI assistance.
- Provide **assistive technologies** for pupils with additional needs, such as text-to-speech, speech recognition, and reading support.

All AI tools must be:

- Approved by the Senior Leadership Team (SLT) and the eSafety Lead.
- Transparent in their operation, with staff and pupils informed about their capabilities and limitations.
- Age-appropriate and accessible to all pupils.
- Subject to regular review for educational value, safeguarding, and ethical compliance.

Risks and Safeguards

Staff and pupils are made aware of AI's limitations, including:

- **Bias and fairness**: AI systems can perpetuate or amplify existing biases if not carefully managed.
- **Accuracy**: AI outputs may contain errors or misleading information and **staff must always review and check the accuracy of AI-generated content before use**.
- **Privacy**: No personal, sensitive, or identifying data about pupils or staff must be input into AI systems without appropriate consent and data protection measures.
- **Plagiarism and academic integrity**: AI-generated work should be appropriately acknowledged, and the misuse of AI to complete assignments dishonestly is prohibited.

Staff Responsibilities

- Ensure AI-generated content is reviewed and validated before use in teaching or administration.

- Do not input personal or sensitive pupil data into AI tools unless fully compliant with GDPR and ICO guidance.
- Maintain professional judgement and uphold academic integrity when using AI.
- Include discussions of AI ethics and use in ongoing staff training.

Pupil Education and Awareness

- Pupils receive age-appropriate education on AI fundamentals, including how AI works, its benefits, risks, and ethical considerations.
- Pupils learn to critically evaluate AI-generated content and understand when and how to seek help or report concerns.
- Curriculum includes discussion on AI's impact on society and encourages responsible digital citizenship.

Data Protection and Legal Compliance

- The school complies with all applicable laws, including the UK GDPR and the Data Protection Act 2018, regarding AI use.
- A Data Protection Impact Assessment (DPIA) is conducted before introducing any new AI tool that processes personal data.
- Contracts and agreements with AI service providers ensure compliance with data protection and children's rights legislation.
- Automated decision-making or profiling that affects pupils is avoided unless transparent, fair, and subject to human review.

Monitoring and Incident Reporting

- The eSafety Lead monitors AI use and any associated safeguarding concerns.
- All AI-related incidents or concerns are logged on CPOMS under the eSafety category.
- Regular reviews ensure AI tools remain safe, effective, and aligned with school values and statutory guidance.

8. Filtering and Monitoring

Filtering is provided by EXA Networks, ensuring reasonable precautions are taken to reduce access to inappropriate or illegal content. However, it is acknowledged that it is not always possible to guarantee that pupils will never be exposed to inappropriate material.

Through comprehensive teaching and support, pupils are equipped to recognise risks online and know what actions to take should they encounter harmful content.

The eSafety Lead receives immediate alerts of any inappropriate access attempts and a daily report from the filtering system to monitor usage and incidents.

All incidents are recorded on CPOMS under the eSafety category for review and action.

9. Access to School Systems and Password Security

- Access to internet and school systems is managed carefully, with appropriate supervision levels.
- Visitor access is granted temporarily and securely when needed.
- Pupils are taught the importance of safe login practices for platforms like Seesaw, MyMaths, and TT Rockstars.
- Staff receive guidance on secure password creation and managing devices used at home and school.
- Personal, sensitive data access is restricted to authorised users only.
- Remote system access requires formal agreements; no unauthorised third-party access allowed.
- Unique user accounts and passwords are issued to all staff and pupils where applicable.
- All users are responsible for keeping their passwords secure and must report any suspected breaches.
- The school maintains logs of user access to monitor and investigate eSafety issues.

10. Use of Communication and Online Publishing

Email

- School-provided email accounts are used for official communications.
- Staff must not use personal email to contact pupils or parents.
- The official parent communication email is admin@barkisland.calderdale.sch.uk.
- Staff are responsible for securing their email passwords and managing inbox storage responsibly.

Publishing Online

- The school maintains editorial control over the website and any official online content.
- Pupils are taught safe and responsible content creation and publication practices.
- Personal data and pupil identities are protected; parental consent is required before publishing images.
- Group photographs are used without names attached.
- Pupils only publish on publicly accessible sites under supervision and with safeguards in place.

11. Use of Images, Video, and Sound

- Parental permission is required for photographs and recordings of pupils.
- Digital media must be appropriate and not include full names or sensitive information.
- Personal mobile phones may be used by staff only for school purposes; images must be uploaded to school systems and deleted promptly.
- Parents may photograph events for personal use only and are reminded not to share images of other pupils online.

12. Video Conferencing and Online Meetings

- Video conferencing enhances learning and is always supervised by staff.
- Pupils do not operate or set up meetings independently.
- Equipment and meeting rooms are secured when not in use.
- Recording requires consent from all participants.
- Meetings between staff and pupils outside school require prior approval and parental awareness.

13. Mobile Phones and Personal Devices

- Pupils are prohibited from using mobile phones during school hours.
- Staff must keep phones silent or off during lessons unless agreed otherwise.
- Personal phones must not be used for direct communication with pupils or parents.
- Secret recording or sharing of images/video on social media without consent is strictly prohibited.
- The Headteacher may examine content on devices if disciplinary breaches are suspected.

14. Other Technologies

- The school regularly evaluates new technologies for educational benefit and safety risks.
- All users must apply school eSafety standards when using personal or new devices, regardless of location.

15. Protecting School Data and Information

- The school is registered under the Data Protection Act 2018 and complies fully.
- Staff receive training on data security and safe handling practices.
- Sensitive data is stored on encrypted devices with strong password protection.
- Procedures ensure secure remote working and data disposal.
- Backups and disaster recovery plans are in place.
- Shared sensitive information is labelled clearly and protected accordingly.

16. Asset Management

- All school hardware and software are inventoried.
- Disposal of equipment follows legal and environmental standards, including certified data destruction.

17. Review and Monitoring

- The policy is reviewed annually or in response to legislation, technology changes, or incidents.
- Input is gathered from stakeholders including staff, pupils, parents, and governors.
- eSafety incidents logged in CPOMS are regularly analysed.

18. Related Policies

This policy complements and should be read alongside:

- Safeguarding and Child Protection Policy
- Behaviour and Anti-Bullying Policy
- Data Protection Policy
- Remote Learning Policy
- Staff and Pupil Acceptable Use Policies

Created September 2025

Children's Acceptable User Agreements

EYFS (Nursery & Reception) – *My Technology Promise*

I will try to:

- Be kind when I use iPads, computers, or other devices.
- Use my hands gently when I touch screens or keyboards.
- Tell a grown-up if something on the screen upsets me.
- Listen when my teacher says it's time to stop.
- Share nicely with my friends.
- Ask a teacher if I don't understand what a computer or robot is saying.

I promise to use technology safely!

KS1 (Years 1–2) – *My Computer Rules*

When I use a computer, tablet, or go online, I will:

- Ask an adult if I'm not sure.
- Be kind with my words and pictures.
- Tell a teacher or parent if I see something that makes me feel sad or worried.
- Keep my passwords and personal information secret.
- Only use websites, apps, and AI helpers (like chatbots) my teacher or parent says are OK.

I agree to follow these rules to keep myself and others safe.

LKS2 (Years 3–4) – *My Online Safety Agreement*

To stay safe and be a good digital citizen, I will:

- Use kind words when I talk or message online.
- Ask permission before going on websites, apps, or using AI tools.
- Never share personal details like my full name, school, address, or passwords.
- Tell a trusted adult if I see anything upsetting or confusing.
- Understand that AI (like chatbots or voice assistants) doesn't always give the right answers — I will ask a teacher if I'm not sure.
- Only use school devices and accounts the way I've been taught.

I promise to be safe, smart, and responsible with technology.

UKS2 (Years 5–6) – *My Digital Responsibility Pledge*

As a confident and respectful internet user, I will:

- Think before I click, post, or share.
- Treat others with respect online, just like in real life.
- Never post or share private information about myself or others.
- Use strong passwords and keep them private.
- Report anything that makes me feel uncomfortable, unsafe, or worried.
- Use AI tools (like chatbots or generators) **only with permission** and **never to cheat or copy** work.
- Understand that not all AI information is correct — I will always check with an adult or teacher.
- Use devices, emails, and learning platforms responsibly and for school tasks.

I understand that how I use technology matters, and I will use it in a safe, fair, and respectful way — including when I use AI.