Online Safety Policy

Serenity School

Author:	COO
Approved by:	Governing Body
Policy Holder:	Headteacher
Date Approved	01.09.2025
Next review due by:	01.09.2026

1. Aims

Our school aims to:

- Maintain robust systems to protect pupils, staff, volunteers, and governors from online risk.
- Identify and support groups of pupils who may be at greater risk of harm online.
- Educate the whole school community about safe, responsible, and positive use of technology, including mobile, wearable, and AI-based tools.
- Establish clear mechanisms for identifying, escalating, and responding to online incidents.

The Four Key Categories of Online Risk

Our approach is based on the DfE's categorisation of online risk:

- **Content:** Exposure to illegal, harmful, or inappropriate content (e.g. pornography, extremist material, deepfakes, or harmful misinformation).
- **Contact:** Harmful online interactions (e.g. grooming, coercion, impersonation, manipulation via AI-generated personas).
- **Conduct:** Personal online behaviour that causes or increases harm (e.g. sharing explicit images, bullying, harassment, misuse of AI tools).
- **Commerce:** Financial risks such as scams, phishing, gambling, and fraudulent use of digital assets.

2. Legislation and Guidance

This policy is based on:

- *Keeping Children Safe in Education* (KCSIE 2025)
- *DfE Filtering and Monitoring Standards* (2023)
- *Working Together to Safeguard Children* (2023)
- *Teaching Online Safety in Schools* (DfE, 2019)
- *Preventing and Tackling Bullying (including Cyber-bullying)* (DfE, 2023)
- *UKCIS Guidance: Sharing Nudes and Semi-Nudes* (2022)
- *DfE Guidance on Searching, Screening and Confiscation* (2024)
- *DfE Advice on Artificial Intelligence in Education* (2025 update)
- Relevant laws: Education Acts 1996–2011, Equality Act 2010, Data Protection Act 2018, UK GDPR.

3. Roles and Responsibilities

3.1 The Governing Board

- Holds overall accountability for online safety, ensuring compliance with KCSIE 2025 and the DfE's filtering and monitoring standards.
- Ensures the school's digital safeguarding arrangements are fit for purpose and reviewed annually.

- Assigns a named Online Safety Governor to oversee compliance (Ebere Emezie, eemezie@serenityschool.org.uk).
- Ensures online safety is embedded across safeguarding, curriculum, and staff development.

Governors must ensure:

- All staff receive annual online safety training and termly updates.
- The school has appropriate filtering and monitoring systems in place that:
    - Block harmful or inappropriate content effectively.
    - Are reviewed at least annually, with logs available for governance.
    - Are proportionate, avoiding unreasonable restriction of teaching and learning.
    - Identify and assign clear roles for managing filtering and monitoring.
    - Are documented through an annual filtering and monitoring review completed by the DSL and ICT provider.

3.2 The Headteacher

- Ensures consistent implementation of this policy and that all staff understand their responsibilities.
- Works with the DSL and ICT provider to ensure technical compliance and safeguarding oversight.

3.3 The Designated Safeguarding Lead (DSL)

The DSL is responsible for the day-to-day leadership of online safety, including:

- Oversight of filtering, monitoring, and online safety incident management.
- Maintaining a termly online safety risk assessment reflecting technological and behavioural changes (e.g. AI misuse, deepfakes, or synthetic media).
- Ensuring all online safety incidents are recorded, escalated, and analysed for patterns and learning.
- Providing regular training updates and contributing data to the school's safeguarding and compliance dashboard.

3.4 The ICT Provider (Techlogic IT Services Ltd)

- Implements and maintains DfE-compliant filtering and monitoring systems.
- Conducts monthly security checks and maintains a log of filtering updates.
- Works with the DSL to ensure all monitoring alerts are reviewed and acted upon.
- Provides an annual written filtering and monitoring report to the DSL and governing board.

3.5 All Staff and Volunteers

All staff, including contractors and volunteers, must:

- Follow this policy and the Acceptable Use Agreements.
- Report concerns, system failures, or breaches immediately to the DSL.
- Seek approval for any temporary bypassing of filtering systems for educational reasons.

- Complete annual online safety and AI-awareness training.

3.6 Parents/Carers

- Ensure their child follows the school's Acceptable Use Agreements.
- Engage with guidance provided by the school on online safety and emerging technologies.

3.7 Pupils

- Follow Acceptable Use Agreements.
- Report any concerns to staff or the DSL immediately.
- Understand that AI tools, social media, and online interactions carry both learning value and risk.

4. Artificial Intelligence (AI) and Emerging Technologies

Serenity Schools recognise the educational benefits of AI and new technologies but also their risks.

Staff and pupils must:

- Use AI tools only for approved educational purposes and within defined parameters.
- Avoid using AI systems to create, share, or manipulate digital content involving real individuals (e.g. deepfakes).
- Report any suspected misuse of AI tools (e.g. fake images, impersonation, or misinformation) to the DSL immediately.
- Be aware that AI platforms may collect, store, or reproduce data entered, which can breach confidentiality or data protection laws.

The DSL and ICT provider will:

- Conduct an annual AI risk assessment evaluating exposure to AI-related risks.
- Ensure that filtering systems recognise and restrict access to unregulated AI platforms where appropriate.
- Provide annual AI-safeguarding training for staff and pupils.

5. Filtering and Monitoring Standards

In line with the DfE Filtering and Monitoring Standards (2023):

- The school ensures that filtering and monitoring systems are technically effective, age-appropriate, and regularly tested.
- Roles and responsibilities are clearly documented (DSL: oversight; ICT Provider: operation; Headteacher: accountability).
- Reviews of filtering and monitoring systems take place at least annually, and logs are retained for governance.
- Systems are configured to:
    - Block access to known harmful sites and material.
    - Alert the DSL automatically to concerning user behaviour.
    - Allow exceptions only through an approved, auditable process.

- The annual filtering and monitoring review will be signed by the Headteacher and DSL and presented to the Governing Board.

6. Monitoring and Review

- The DSL logs all online safety incidents and reviews emerging patterns every term.
- An annual risk assessment will be completed to reflect technological changes, including AI-related threats.
- The Headteacher and Online Safety Governor will review this policy annually and following any national DfE or UKCIS update.

7. Links with Other Policies

This policy should be read alongside:

- Child Protection and Safeguarding Policy
- Behaviour for Learning Policy
- Staff Code of Conduct
- Mobile Phone and Device Policy
- Data Protection and GDPR Policy
- ICT Acceptable Use Agreements (Staff, Pupils, Parents)
- Filtering and Monitoring Annual Review Report