POLICY

# Online Safety

**Formulation date:** January 2016

**Reviewed:** April 2026

**Next review date:** March 2028

**Senior leader responsible:** Principal

**Statement of intent**

Casterton College Rutland recognises that online safety is an integral part of safeguarding and promoting the welfare of children. The use of digital technology is embedded across the life of the school and plays a significant role in teaching, learning, communication and school operations. As such, robust measures are in place to protect students and staff from harm and to promote safe, responsible and informed use of technology.

Safeguarding concerns may present differently online; however, they are assessed and responded to using the same principles and procedures as offline concerns. All staff understand that harm can occur both in and outside school, during and beyond the school day, and that children may be vulnerable to abuse from peers or adults online.

Online safety risks are categorised using the 4Cs framework:

- **Content** – exposure to illegal, inappropriate or harmful material.
- **Contact** – harmful interaction with others online, including grooming or exploitation.
- **Conduct** – personal online behaviour that increases the likelihood of harm.
- **Commerce** – risks relating to fraud, scams, gambling or financial exploitation.

This policy sets out how the school manages these risks through education, prevention, monitoring and effective response.

**Legal framework**

This policy has due regard to relevant legislation and statutory guidance including:

- Keeping Children Safe in Education (DfE, 2024)
- UK GDPR and Data Protection Act 2018
- Voyeurism (Offences) Act 2019
- Filtering and monitoring standards for schools and colleges (DfE, 2024)
- Teaching online safety in school (DfE, 2023)
- Generative artificial intelligence in education (DfE, 2023)

Education for a Connected World (UKCIS, 2020)

This policy operates alongside, and should be read in conjunction with, other safeguarding and behaviour-related policies, including the Child Protection and Safeguarding Policy, Behaviour Policy, Staff Code of Conduct, Student Mobile Phone Policy and Cyber Security Policy.

**Roles and responsibilities**

**Governing board**

The governing board has strategic oversight of online safety and will:

- Ensure this policy complies with statutory guidance.
- Ensure online safety is embedded within the safeguarding framework.
- Ensure appropriate filtering and monitoring systems are in place and reviewed at least annually.
- Ensure staff receive regular safeguarding and online safety training.
- Receive regular updates on online safety from senior leaders.

**Principal**

The principal will:

- Ensure online safety is fully embedded across school policies, procedures and curriculum.
- Ensure staff are appropriately trained and supported.
- Promote a whole-school safeguarding culture including digital safety.
- Work with governors and the DSL to ensure this policy is reviewed annually.

**Designated Safeguarding Lead (DSL)**

The DSL has lead responsibility for online safety and will:

- Coordinate the school's approach to online safety.
- Ensure filtering and monitoring concerns are escalated appropriately.
- Maintain secure and accurate records of online safety incidents.
- Monitor trends and emerging risks.
- Liaise with external agencies where required.
- Provide termly updates to governors.

**IT support staff**

IT technicians will:

- Maintain effective filtering and monitoring systems.
- Support safeguarding staff in investigating concerns.
- Keep systems secure and up to date.

**All staff**

All staff will:

- Model safe and professional online behaviour.
- Remain vigilant to indicators of online harm.
- Report concerns immediately in line with safeguarding procedures.
- Ensure online safety messages are reinforced through the curriculum where relevant.

**Students**

Students are expected to:

- Follow school policies relating to technology use.
- Seek help if they are worried about online content or behaviour.

- Report concerns about their own or others' online safety.

**Whole-school approach to online safety**

Online safety is embedded through:

- Regular safeguarding and online safety training for staff and governors.
- Curriculum provision including RSHE, PSHE and computing.
- Assemblies and targeted interventions.
- Active monitoring of digital systems.
- Engagement with parents and carers.

**Handling online safety concerns**

All online safety concerns are managed in accordance with the Child Protection and Safeguarding Policy. Staff do not promise confidentiality and understand that information may need to be shared to protect students from harm.

The school recognises that harmful online behaviour exists on a continuum and that early and proportionate intervention is essential. Students displaying harmful behaviour may themselves be vulnerable and will be supported accordingly.

All incidents are recorded by the DSL and reviewed to identify patterns or areas for improvement.

**Use of smart technology and mobile phones**

The school operates a highly restrictive mobile phone policy to reduce risk and support pupil wellbeing.

- students may bring mobile phones to school but must secure them in school-issued mobile phone pouches (e.g. Yondr) upon arrival.
- pouches remain locked throughout the school day and are unlocked only at the end of the day, unless an exception is authorised by staff for safeguarding or medical reasons.
- students do not have access to mobile phones during lessons, social times or transitions.

This approach supports safeguarding, reduces distraction and minimises the risk of online harm during the school day. Any misuse of smart technology is managed in line with the Behaviour Policy and Student Mobile Phone Policy.

**Generative artificial intelligence (AI)**

The school recognises that generative AI tools are increasingly accessible and may present both opportunities and safeguarding risks.

The school will:

- Educate students on safe, ethical and age-appropriate use of AI.
- Teach students to recognise misinformation, bias and over-reliance.
- Prohibit use of AI that breaches academic integrity, copyright or assessment rules.
- Ensure personal or sensitive data is not entered into AI tools.
- Apply filtering and monitoring to limit access to inappropriate AI platforms where practicable.

Staff will:

- Model transparent and responsible use of AI.
- Not use AI tools to make safeguarding, pastoral or assessment decisions about students.
- Misuse of AI will be addressed in line with behaviour and disciplinary procedures.

**Filtering and monitoring**

The school meets the DfE's filtering and monitoring standards. Named staff are responsible for oversight of these systems and understand how safeguarding concerns identified through monitoring are escalated.

Systems are:

- Appropriate to students' age and needs.
- Regularly reviewed and updated.
- Used proportionately, with users informed about monitoring.

Deliberate attempts to bypass filtering are treated as safeguarding concerns and managed accordingly.

**Remote learning**

Remote learning is delivered in line with the Remote Education Policy. Staff remain alert to safeguarding risks including online behaviour, inappropriate communication and pupil engagement, and concerns are reported promptly.

**Educating parents**

We work in partnership with parents to promote online safety. Support is provided through newsletters, guidance and signposting to trusted resources. Parents are encouraged to reinforce safe online behaviours at home and to engage with school policies.

**Monitoring and review**

This policy is reviewed annually and following any significant online safety incident. Updates are communicated to staff, students and parents. Online safety practice is evaluated as part of the school's wider safeguarding monitoring and self-evaluation.