

ONLINE SAFETY & E-SAFETY



Rachel Hart
Stacey Hickey

STRIVE Inclusive
Academy

Approved
July 2024

Review Date
July 2025



Aims

This policy has been written by Strive IA involving staff, building on The Education People policy template, with specialist advice and input as required. It takes into account the DfE statutory guidance 'Keeping Children Safe in Education 2023', Early Years and Foundation Stage, 'Working Together to Safeguard Children' and the local Safeguarding Children Multi-Agency Partnership procedures.

We recognise that online safety is an essential part of safeguarding and acknowledge our duty to ensure that all pupils and staff are protected from potential harmful and inappropriate online material and/or behaviour. This policy sets out our Provisions' approach to online safety which will empower, protect and educate our pupils and staff in their use of technology and establishes the mechanisms in place to identify, intervene, and escalate any concerns where appropriate.

To support schools and alternative provisions to meet this duty, the Department for Education has published filtering and monitoring standards which set out that schools should:

- Identify and assign roles and responsibilities to manage filtering and monitoring systems.
- Review filtering and monitoring provision at least annually.
- Block harmful and inappropriate content without unreasonably impacting teaching and learning.
- Have effective monitoring strategies in place that meet their safeguarding needs.

Governing bodies and proprietors should review the standards and discuss with IT staff and service providers what more needs to be done to support schools and colleges in meeting this standard. The Prevent duty Departmental advice for schools and childcare providers and Home Office Statutory guidance: Prevent duty guidance.

Strive IA understands that breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- **Contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, for example, consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying.
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams.



Strive IA recognises that students are at risk of abuse online as well as face to face. In many cases abuse will take place concurrently via online channels and in daily life. Children can also abuse other children online.

This policy applies to Students, parents and carers and all staff, including the Proprietors, leadership team, teachers, support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the Provision.

Strive IA identifies that the internet and technology, including computers, tablets, mobile phones, smart watches, games consoles and social media, is an important part of everyday life, and presents positive and exciting opportunities, as well as challenges and risks.

This policy applies to all access to and use of technology, both on and offsite.

Strive IA recognise that children may not feel ready or know how to tell someone that they are being abused, exploited, or neglected online, and/or they may not recognise their experiences as being abusive or harmful. This should not prevent staff from having professional curiosity and speaking to a DSL if they have any online safety concerns about a child.