H.G.S
Reflect, Believe,
Develop: Achieve!

Hidelow Grange School Online Safety Policy

Juliet Smith – Deputy Headteacher Deputy DSL

Benjamin Neasom Headteacher – DSL

Rob McConomy – Regional Lead

Written:	**March 2026**
Author:	**Benjamin Neasom, Headteacher**
Reviewed:	**March 2026**
Next Review:	**March 2027**
Approved by:	**Rob McConomy**

1. Purpose

Hidelow Grange School recognises both the significant benefits and inherent risks of technology use among our pupils, who present with harmful sexual behaviours (HSB) and complex social, emotional and mental health (SEMH) needs.

This policy aims to:

• Safeguard pupils from harmful or inappropriate online content, with particular attention to sexual content, grooming, and exploitation given our HSB cohort
• Promote a whole-school approach to online safety that integrates with our therapeutic and trauma-informed practice
• Balance access control with education on responsible use, recognising that our pupils require higher levels of supervision and support
• Empower pupils to make safe decisions online and report concerns without fear
• Ensure staff understand online-safety practices specific to working with pupils who present with HSB
• Protect staff from allegations and ensure professional boundaries are maintained

An effective whole-school approach to online safety empowers, protects and educates pupils in their use of technology and establishes robust mechanisms to identify, intervene in, and escalate any concerns appropriately.

2. Legislative Context

This policy is underpinned by statutory and regulatory frameworks which ensure our pupils are protected from harm and risks arising from digital technologies:

Keeping children safe in education 2025

Teaching online safety in schools - GOV.UK

Online safety (e-safety) and schools | NSPCC Learning

Working together to safeguard children 2023: statutory guidance

Data Protection Act 2018

Counter-Terrorism and Security Act 2015

Education Act 2011

Education and Inspections Act 2006

This policy should be read alongside:

• Safeguarding & Child Protection Policy
• Anti-Bullying Policy
• Behaviour Policy
• Data Protection Policy

• Staff Code of Conduct
• Acceptable Use Agreements (Staff and Pupils)

This Policy is underpinned by a range of statutory and regulatory frameworks which ensure our children and students are protected from harm and risks arising from digital technologies. They include:

3. Background

Our School:
Hidelow Grange School is an independent specialist SEMH residential school for boys aged 11-18 who are Looked After Children. We provide education for up to 20 pupils who present with harmful sexual behaviours (HSB) and complex interpersonal, emotional and behavioural needs.

Our Pupils:
All pupils have experienced significant trauma, loss and disrupted care/education histories. Many have fragile self-esteem, attachment difficulties, and challenges forming appropriate relationships. **Crucially, all pupils present with harmful sexual behaviours, which significantly increases online safety risks including:**

- **Accessing, creating or sharing sexual content online**
- **Using technology to perpetrate sexual harm (e.g., sexting, online grooming of others)**
- **Vulnerability to online sexual exploitation and grooming**
- **Compulsive or problematic use of pornography**
- **Using technology to bypass supervision or engage in inappropriate sexual communication**

Our Approach: Given this context, **our online safety approach is more restrictive than mainstream schools**, with constant 1:1 supervision, robust filtering/monitoring, and integration with therapeutic interventions addressing HSB.

Technology brings many benefits but also significant risks, particularly for our vulnerable cohort:

Content Risks:

- Exposure to pornography, violent or extreme sexual content
- Fake news, misinformation, conspiracy theories
- Radicalisation and extremist content
- Self-harm and suicide content

Contact Risks:

- Online grooming and sexual exploitation
- Being groomed to perpetrate harm against others
- Inappropriate contact with adults or peers
- Commercial advertising and scams

Conduct Risks:

- **Creating, sharing or requesting sexual images (sexting)**
- **Using technology to perpetrate sexual harm or harassment**
- **Accessing illegal content (child sexual abuse images)**
- Cyberbullying (as victim or perpetrator)
- Sharing personal information inappropriately
- Plagiarism and copyright infringement

AI-Associated Risks:

- AI-generated sexual content or deepfakes
- Using AI tools to bypass filters
- Misinformation appearing credible

HSB-Specific Risks:

- **Re-enacting harmful sexual behaviours online**
- **Using technology to access victims**
- **Normalising harmful sexual attitudes through online content**
- **Triggering or escalating HSB through exposure to sexual content**

4. Roles and Responsibilities

Designated Safeguarding Lead (DSL)

- Leads on safeguarding and online safety
- Oversees incident logs, filtering & monitoring systems, and staff training
- **Is trained in online safety and understands risks including grooming, radicalisation, online abuse and AI.**

Head of Service

- Ensures safety of individuals and staff
- Provides CPD for staff on online safety
- Monitors internal safety roles and reports to governance board

Senior Leadership Team

- Manages daily online safety issues
- Reviews policies and incidents
- Liaises with IT, Local Authority, and external agencies

Information Governance and IT Leaders / Technical Staff

- Maintains secure infrastructure and filtering systems
- Monitors network/VLE/email use
- Implements and updates monitoring software
- **Ensures wireless access is proactively managed and secured**

All Staff

- Stay informed on online safety and peer-on-peer abuse
- Follow the Acceptable Use Policy (GIG 18 Policy)
- Report concerns to the Online Safety Lead
- Maintain professional communication via official systems
- Embed online safety in curriculum and activities
- **Never share login credentials**
- Monitor device use and internet access

Parents/Carers

- Play a key role in promoting safe technology use
- **Our school/college supports parents via newsletters, events and campaigns**

5. Teaching and Learning

Individuals are given clear objectives, taught acceptable use and guided in evaluating online materials.

Our School/College:

- Complies with copyright laws
- Provides age-appropriate access
- Maintains virus protection and system security
- **Ensures password management and IT security align with the Prevent Policy**

6. Use of Email

Staff use work-provided email accounts for all official communication. **This protects confidentiality and staff from allegations.**

7. Website

Our website only publishes location contact details (address, email, phone) and does not publish personal information of staff or individuals will be shared. All content is accurate, appropriate, and complies with privacy and copyright policies. **No photographs of children or students are uploaded or shared without appropriate consent.**

8. Internet Use

- Inappropriate website content is reported immediately
- Parents/carers are informed that internet access is supervised
- Every individual has a personalised online safety risk assessment that is reviewed regularly in line with care and education planning
- **Our School/College has robust filtering and monitoring systems in place, however, staff are aware that mobile devices with wireless access can bypass these systems – staff remain alert to any signs of concern**

9. Social Networks

Teaching staff deliver lessons on social networking safety, covering areas such as the risks of uploading personal content and challenges removing content once shared.

Lessons also focus on privacy and the risks surrounding sharing personal details. This is pitched to children and students' development and level of understanding.

10. Staff and Volunteers

- Follow the GHR 37 Code of Conduct and Teams Etiquette Guide
- Raise concerns about inappropriate use
- **Follow the Whistleblowing, Child Protection and other associated policies**
- Immediately reporting concerns when they arise
- Maintain confidentiality and involve parents/carers when appropriate

11. Sexting (Sharing Nudes and Semi-Nudes)

Sexting, also known as the sharing of nudes or semi-nudes, involves sending or receiving sexually explicit images, videos, or messages via digital devices. **While often perceived as harmless, it is illegal for anyone under 18 to create, share, or possess such content—even if consensual.** Young people may engage in sexting for reasons such as peer pressure, curiosity, or self-esteem, but they often underestimate the risks, including loss of control over images, exposure to exploitation, bullying, and emotional distress. Once shared, content can be copied, distributed, or accessed by unknown individuals, including sex offenders.

Staff must respond to disclosures calmly and follow safeguarding procedures immediately. **This involves notifying the DSL within one hour**. The National Police Chief's Council (NPCC) advises that safeguarding—not criminalisation—should be the priority. If the incident involves coercion, violence, or individuals under

13 or over 18, police and children's social care must be contacted**. If a child is in immediate danger, call 999 or NSPCC at 0808 800 5000. Staff should avoid viewing the content and isolate devices if necessary.** All actions must be recorded, and if a child is in immediate danger, emergency services must be contacted without delay.

12. Use of Digital Images and Videos

- Staff educate individuals on risks of sharing images
- Staff only use school/college equipment for capturing images
- Staff ensure individuals are appropriately dressed prior to taking an image
- **Full names are avoided in published photos**
- **Images are carefully selected and follow best practice guidance**

13. Cyberbullying

- Cyberbullying is persistent, anonymous, and harmful
- Common forms include texts, images, emails, chat rooms, IM, websites
- Cyberbullying can reach large audiences quickly and anonymously
- Most incidents involve peers within the same class or year group
- Despite lack of physical evidence, cyberbullying can be deeply harmful
- **Our School/College supports victims and educates staff and individuals on prevention and reporting**
- **Regular parent/carer sessions are held on cyberbullying and online child protection**

14. Emerging Technology - AI

Our School/College evaluates emerging technology for suitability before use. AI-generated content is now recognised as a potential online safety risk. Our School/College is aware that children/students may encounter misinformation, disinformation, or harmful outputs from AI tools — even those used in educational settings. Filtering and monitoring systems are reviewed to account for AI risks and our digital safety infrastructure is in line with the new DfE guidance/tool 'Plan Technology for Your School'.

Our Designated Safeguarding Leads (DSLs) is alert to AI-related risks including how AI tools might be used to bypass filters, spread conspiracy theories, or deliver content that appears trustworthy but is inaccurate or harmful.

Our school staff are trained in AI risks so they can identify and respond to any emerging concerns.

15. Management of Information Systems

All systems are managed according to the Information Security Policy. Virus protection is updated daily and robust filtering and monitoring systems are in place. Unsuitable sites are blocked immediately, servers are secured, access is restricted and files are checked for malware. Software is installed by IT technicians and staff **never share assigned devices or login credentials. Wireless access is proactively managed and secured.**

16. Students aged 18 years and Over

Online safety responsibilities extend to students aged 18 and over, especially those who may be vulnerable due to trauma, learning disabilities, mental health conditions, or other needs. Although legally classified as adults, these individuals may still require tailored safeguarding measures, including supervised access to technology, individualised risk assessments, and ongoing education around online safety.

Staff are alert to signs of online abuse, exploitation, or coercion, and where there are concerns about an individual's ability to make informed decisions, staff follow the Over 18s Safeguarding Policy and arrange for Mental Capacity Act (MCA) assessments where appropriate. In such cases, decisions are made in the individual's best interests, ensuring that support and restrictions are proportionate, protective, and respectful of individual rights.

Review History

A review will be undertaken annually as a minimum. However, subject to a significant safeguarding concern this policy and all other attached policies will be reviewed and monitored as part of a lessons learned review.

This policy was reviewed in August 2025 by Laura Dickie (Head of Policy), Kate Brogan (Head of IT), Nico Putter (Group Head of Cyber and Information), Russell Edge (Senior Information Risk Owner), the DSL of the School and agreed by the Head of the Governance Board.

Next Review – September 2026