HIDELOW GRANGE SCHOOL

Safeguarding Policy Suite

Filtering and Monitoring of Digital Technology

Approved by:	B. Neasom, Headteacher & DSL
Date approved:	June 2026
Last reviewed:	June 2026
Next review due:	September 2026
Reviewed by (CareTech):	Laura Dickie, Jo Dunn, Kate Brogan, Russell Edge, August 2025

Designated Safeguarding Lead	Deputy DSL	Regional Lead
B. Neasom	**J. Smith**	**R. McConomy**
Headteacher & DSL	Deputy Headteacher	CareTech Regional Lead

Introduction

This policy is written in line with:

- Keeping Children Safe in Education (KCSiE) 2025
- Meeting Digital and Technology Standards in Schools and Colleges (updated May 2024)
- Appropriate Filtering and Monitoring guidance from the UK Safer Internet Centre
- DfE filtering and monitoring standards for schools and colleges

This policy is also written for students over 18 years and is in line with the Care Act 2014, Mental Capacity Act 2005 and Education Act 2002.

Per KCSiE 2025 Annex C, filtering and monitoring measures are integrated into the school's safeguarding framework and reviewed termly.

This policy is supported by the following wider policies:

- Child Protection Policy
- Child on Child Abuse Policy
- Role of the DSL
- Missing from Education
- Absent from Education Policy
- Schools Safer Recruitment Policy
- Online Safety Policy
- Behaviour Policy
- PREVENT Policy

- SEND Policy
- Staff Behaviour Policy / Code of Conduct

Purpose

Hidelow Grange School is committed to safeguarding and promoting the welfare of children and students by providing a safe environment in which to learn. This policy ensures school staff do all they reasonably can to limit pupils' exposure to online risks from the school's IT systems.

This policy ensures the leadership team and relevant staff have an awareness and understanding of the provisions in place, manage them effectively and know how to escalate concerns when they arise. Governing bodies and proprietors also consider the number and age range of their children, those potentially at greater risk of harm, how often they access the IT system and the proportionality of costs against safeguarding risks.

Aims of this policy

- To ensure that risks linked to digital and technology equipment are assessed
- Staff are aware of the need to filter and monitor content
- Staff know how to use the filtering and monitoring equipment
- Individuals are protected from viewing inappropriate or harmful content
- Staff know how to report concerns to the DSL
- The DSL has clear monitoring checks in place and knows how to escalate concerns
- All staff complete annual online safety training as mandated by KCSiE 2025

What is filtering?

Filtering, applied to digital and technology equipment, is a way of allowing people to access some content while blocking other types of content. The school's filtering system blocks harmful and inappropriate content without unreasonably impacting teaching and learning, in line with the DfE's Meeting Digital and Technology Standards 2024. Filtering configurations use dynamic URL categorisation and multiple filtering layers.

What is monitoring?

Monitoring means observing and checking the quality or progress of something over a period of time. Schools can monitor devices in a number of ways:

- Physically monitoring by staff watching screens
- Live supervision by staff on a console with device management software
- Network monitoring using log files of internet traffic and web access
- Individual device monitoring through software or third-party services

What are the risks?

Research by the Office for National Statistics found that almost nine in ten children (89%) aged 10 to 15 go online every day, and around one in six (17%) spoke with someone they had never met before in the previous 12 months. Digital media and technology have become embedded in society and are useful aids to extend children's learning, but they bring attached risks.

The risks children and students face online include access to:

- Pornography or inappropriate sexualised content
- Violent pranks or content depicting harm caused to others
- Radical content or ideologies inconsistent with British values
- Content relating to self-harm or suicidal ideologies
- Online or cyberbullying

- Exploitation and grooming linked to radicalisation, child sexual exploitation, criminal exploitation or modern slavery
- Child on child / student on student abuse and pressures to share youth produced sexual imagery

What filtering and monitoring systems are in place?

Hidelow Grange School uses Fortinet security. The filtering system is Fortigate and the monitoring system is Fastvue.

Fortigate filters harmful content and protects users from spam and malware attacks. Fastvue is a tool that alerts the nominated person to online searches completed by children, highlighting searches it considers harmful or inappropriate and sending live alerts to the person responsible for oversight of filtering and monitoring.

The filtering system can be tested to give staff an overview of its effectiveness using the SWGfL Test Filtering tool. Filtering is tested at least termly on both staff and student accounts.

The role of staff

When using IT equipment, staff remain vigilant and risk assess the use of devices and digital technology, considering:

- The vulnerability of each pupil or student
- Any known risks with individual children or students, including risks of radicalisation, CSE, criminal exploitation or bullying
- Whether there are individuals within the group who can be easily influenced by others

Staff consider the purpose of using digital technology and whether the educational advantage will outweigh the potential of exposing a child or student to harmful content. Staff support children and students to access the internet safely and discuss risks and measures. Staff inform children and students that they can report inappropriate content, including confidentially if required.

Staff report any concerns about harmful or inappropriate content seen or suspected to have been accessed to the DSL immediately.

KCSiE groups online safety risks into four areas: content, contact, conduct and commerce (sometimes referred to as contract), known as the 4 Cs. Staff have these in mind when considering what pupils and students are accessing online.

The role of the DSL and other identified staff

The DSL ensures processes are in place to enable effective filtering and monitoring practices and must complete annual training in digital safeguarding and monitoring.

In line with DfE standards, the school:

- Identifies and assigns roles and responsibilities to manage filtering and monitoring systems. A designated Online Safety Lead is in place
- Reviews filtering and monitoring provision at least annually, including identification of gaps, technical limitations, detailed assessments of vulnerable student groups (those with SEND or EAL) and the impact of new technologies, particularly generative AI. Reviews include an independent audit and feedback report to the proprietor
- Blocks harmful and inappropriate content without unreasonably impacting teaching and learning, in line with recommended blocklists. Blocklists are updated immediately to capture emerging threats
- Maintains effective monitoring strategies including keyword and image-based detection, with daily alerts and weekly DSL reviews

The school also has a locality risk assessment in place which takes account of Prevent risks alongside a Prevent action plan.

The DSL ensures the above tasks are allocated to a nominated person with the required knowledge, skills and experience. That person holds a certificated qualification in online safety management (NCSC Schools Guidance 2024).

The DSL monitors immediate alerts to keep abreast of patterns and trends in searches and passes on concerns for actioning. Alerts are triaged within 24 hours, logged and retained for 12 months.

The DSL works closely with the IT department to ensure that systems function technically and align with broader safeguarding strategies. If monitoring raises concerns about gaps in filtering, the DSL liaises with the Group Head of IT (Kate.Brogan@cambiangroup.com) to ensure risks are reduced.

When incidents occur which could relate to child on child or student on student abuse (such as youth produced sexual imagery, cyberbullying or harmful sexual content), the DSL refers to the Child on Child / Student on Student Abuse Policy and, where necessary, the Child Protection / Adult Safeguarding Policy.

Staff use of mobile phones and devices

Staff are not permitted to carry personal mobile phones during teaching time. Mobile phones must not be left on any office desk and are kept in a safe location on silent mode. The school's mobile phone policy (Policy 40.00) applies at all times. Staff are also expected to:

- Use business internet filtering and monitoring systems to minimise exposure to inappropriate material
- Sign an Acceptable Use Agreement annually
- Not use, move or remove IT equipment without the express permission of relevant staff
- Not share network access credentials with any other person
- Not intentionally visit internet sites that contain obscene, violent, illegal, hateful or otherwise objectionable material
- Complete e-safety training or education refreshed at least annually
- Not upload or download non-approved software

Usage logs are retained for a minimum of six months (DfE 2024). CareTech reserves the right to check a service user's personal technology for inappropriate or malicious content, with this being expressly communicated to individuals and relevant professionals.

Visitor use of mobile phones and devices

Visitors are not to be left alone with children unless previously agreed by the Headteacher or DSL. Staff know visitors' whereabouts at all times. Visitors must not make direct contact with children or students met in school by phone, email, letter or social network sites, and must not take photographs of children or students.

Pupils and students: use of mobile phones and devices during the school day

Pupils and students do not use mobile phone devices during the school day unless agreed with the Headteacher as part of an individual support plan.

Pupils and students: use of mobile phones and devices outside of education hours

Pupils and students may use their phones outside of educational hours. They are encouraged to use the school wifi so that content can be monitored. Staff remain vigilant, and those with a history of known risks have an up-to-date risk assessment under review. If concerns regarding content accessed by a child or student emerge, staff inform the DSL. Any change in presentation that gives cause for concern is addressed via the Child on Child Abuse / Student on Student Abuse Policy and the Child Protection / Adult Safeguarding Policy.

Use of mobile phones and devices on off-site excursions

Off-site risk assessments include mobile-device controls and logging procedures. Please refer to the school's risk assessment and off-site activities policy for further guidance.

Review history

A review will be undertaken annually as a minimum. Subject to a significant safeguarding concern, this policy and all 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), Jo Dunn (Director of Compliance, Quality and Regulation – Children), Kate Brogan (Head of IT), Russell Edge (Senior Information Risk Owner / DPO) and the DSL. It was adopted and adapted for Hidelow Grange School in June 2026 by B. Neasom (Headteacher and DSL).

Next review: September 2026.