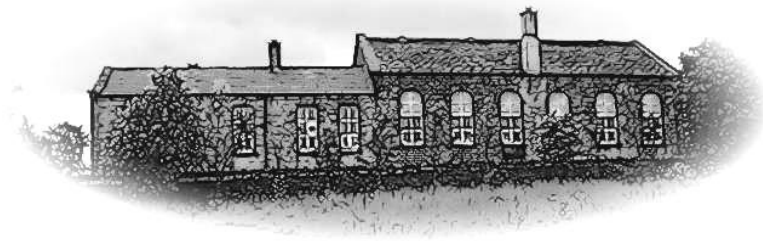


Scapegoat Hill J & I School



School Road, Scapegoat Hill, Huddersfield HD7 4NU
Telephone: 01484 647008, Email: office@scapegoathill.co.uk
Website: www.scapegoat-hill.kirklees.sch.uk
Headteacher: Miss Natalie Shackleton

Online Safety Risk Assessment

Approved by: **Governors**

Date: **July 2026**

Last Reviewed on: **July 2026**

Review Date: **July 2027**

Designated Safeguarding Lead (DSL) and Online Safety Lead: Natalie Shackleton

1. Purpose & Scope – Online Safety

Keeping children safe online is an important part of our school's safeguarding responsibilities. This Online Safety Risk Assessment explains how we protect pupils when they use digital technology in school and during online learning.

The school follows UK government guidance, including:

- Keeping Children Safe in Education (KCSIE)
- Department for Education (DfE) Online Safety Guidance, including advice on social media, harmful content, and emerging technologies such as artificial intelligence (AI)

We regularly review how children use the internet, digital devices and learning platforms. This includes websites, apps, email and online communication tools.

The assessment looks at possible risks, such as access to inappropriate content, online bullying, misinformation and unsafe online behaviour. It also explains the steps the school takes to reduce these risks and help children use technology safely and responsibly.

EYFS and SEND

Children in the Early Years and pupils with Special Educational Needs and Disabilities (SEND) may find it harder to understand online risks. For this reason, online activities for these children are carefully planned, closely supervised and age-appropriate.

Children are taught simple messages, such as telling a trusted adult if something online makes them feel worried or unsafe. Support is adapted to meet individual needs.

Review and Monitoring

This risk assessment is reviewed every year, or sooner if new risks or technologies emerge. Any online safety concerns are managed through the school's safeguarding procedures. Governors are informed of significant online safety matters to make sure arrangements remain effective.

How This Links to Other School Policies and Government Guidance

Online safety is part of our wider safeguarding approach and is supported by national guidance and school policies, including:

Government Guidance

- Keeping Children Safe in Education (DfE)
- DfE Online Safety Guidance
- DfE Using Technology in Schools
- UK Safeguarding legislation and expectations for schools

School Policies

- Safeguarding and Child Protection Policy
- Anti-Bullying Policy (including cyberbullying)
- Acceptable Use Agreements
- Behaviour Policy
- Data Protection and Privacy Policies

This assessment applies to:

- School-owned devices (e.g. iPads, Chromebooks, laptops)
- Internet access provided by the school
- Online learning platforms and cloud services
- Staff and pupil use of technology
- Use of school systems both on-site and off-site

Technology Environment

- Devices used: laptops, Ipads, printers, PCs
- Operating systems: Windows 11
- User accounts: Microsoft 365

Internet filtering solution:

The school uses a WatchGuard Firewall, which through its Unified Threat Management (UTM) features manages web filtering levels, blocks inappropriate and harmful websites, and enforces age-appropriate access controls in line with DfE requirements.

Monitoring and safeguarding solution:

The school uses the Senso Safeguarding application to monitor device activity, identify potentially concerning behaviour, and generate safeguarding alerts to support early intervention by the Designated Safeguarding Lead.

Remote / home learning used: Yes / No

Risk Assessment

Risk Scoring:

- Likelihood: Low / Medium / High
- Impact: Low / Medium / High
- Residual Risk: Risk remaining after controls are applied

1. Access to Inappropriate Content

Pupils may access age-inappropriate, harmful, or illegal content online.

- Commercial – adverts, spam, sponsorship, personal info
- Extremist - violent / hateful content
- Sexual - pornographic or unwelcome sexual content
- Values – bias, racist, misleading info or advice

Controls in place:

- WatchGuard Firewall UTM filtering enforces age-appropriate content categories
- Blocking of harmful and inappropriate websites at network level
- SafeSearch and restricted modes enabled where available
- Staff supervision during device use
- Pupil and parent Acceptable Use Policies in place

Likelihood: Low

Impact: High

Residual Risk: Low

Further actions required:

- Regular review of filtering policies
- Periodic testing of filtering effectiveness

2. Contact Risks (Grooming and Inappropriate Contact)

Pupils may be exposed to inappropriate contact through online platforms, messaging tools, or games.

- Aggressive - being bullied, harassed or stalked
- Sexual – harassment, meeting strangers, being groomed
- Values – self harm, unwelcome persuasions

Controls in place:

- Messaging, social media, and inappropriate communication platforms restricted via WatchGuard filtering
- Senso Safeguarding monitors searches and on-device activity
- Safeguarding alerts are escalated promptly to the DSL
- Staff trained to recognise online safeguarding indicators

Likelihood: Low

Impact: High

Residual Risk: Low

3. Online Conduct (Bullying and Misuse)

Pupils may engage in cyberbullying or misuse online tools.

- Commercial – Illegal downloading, hacking, gambling, financial scams, terrorism
- Aggressive - being bullied, or harassing others
- Sexual – peer harassment, creating and uploading inappropriate material
- Values – providing misleading info or advice

Controls in place:

- Behaviour and Anti-Bullying Policies explicitly cover online conduct
- Online safety education embedded within PSHE and Computing curricula
- Senso Safeguarding supports identification of concerning behaviour
- Incidents logged and managed in line with safeguarding procedures

Likelihood: Medium

Impact: Medium

Residual Risk: Low

4. Self-Harm and Suicide Content

Pupils may encounter content relating to self-harm or suicide.

- Contractual arrangements that may be unfair or exploitative, or which pose security or safety or privacy risks

Controls in place:

- WatchGuard filtering blocks known harmful content categories
- Senso Safeguarding alerts for concerning keywords and activity
- Immediate escalation to the DSL in line with the safeguarding policy

Likelihood: Low

Impact: High

Residual Risk: Low

5. Radicalisation and Extremism

Pupils may be exposed to extremist or radicalising material online.

Controls in place:

- WatchGuard filtering aligned with the Prevent Duty
- Monitoring of searches and device activity through Senso
- Staff trained on Prevent indicators and reporting routes

Likelihood: Low

Impact: High

Residual Risk: Low

6. Data Protection and Privacy

Personal or sensitive data may be accessed, shared, or stored insecurely.

- Data Protection – data loss or compromised
- Security Intrusion – information or access is compromised e.g. hack or virus/malware

Controls in place:

- Use of secure, GDPR-compliant cloud platforms
- Role-based access controls
- Staff training on data protection and information security

Likelihood: Low

Impact: High

Residual Risk: Low

6. Staff Use of Technology

Inappropriate or unsafe use of online systems by staff.

Controls in place:

- Staff Acceptable Use Policy in place
- Monitoring of staff activity in line with policy and data protection requirements
- Clear disciplinary procedures where misuse is identified

Likelihood: Low

Impact: Medium

Residual Risk: Low

7. Emerging Technologies (Including Artificial Intelligence)

Misuse of AI tools or exposure to inappropriate AI-generated content.

Controls in place:

- Access to AI tools managed and restricted where appropriate
- Searches and device activity monitored via Senso
- Staff guidance provided on appropriate and safe use of AI technologies

Likelihood: Medium

Impact: Medium

Residual Risk: Medium

Further actions required:

- Annual review of AI guidance
- Policy updates in line with evolving DfE advice

Incident Response

- All online safety incidents are logged and reviewed
- Safeguarding alerts generated by Senso are investigated promptly
- The DSL escalates concerns in line with the school's Safeguarding and Child Protection Policy
- Parents and external agencies are informed where appropriate

Review and Governance

This Online Safety Risk Assessment is reviewed at least annually
Reviewed following any significant safeguarding or online safety incident

Approved and signed off by senior leadership

Headteacher: _____

Designated Safeguarding Lead: _____

Date: _____

Linked Policies

- Safeguarding and Child Protection Policy
- Behaviour Policy
- Anti-Bullying Policy
- Acceptable Use Policies/Agreement (Staff, Pupils and Parents/Cares)
- Data Protection Policy
- Online Safety Policy

Policy Implemented	July 2026	Headteacher
Policy Reviewed		
Policy Reviewed		