HUNTS CROSS PRIMARY SCHOOL

Online Safety Risk Assessment

Academic Year 2026–2027

Children • Staff • Devices • Networks • Online services

1. Assessment details

Field	Details
School	Hunts Cross Primary School, Liverpool
Assessment owner	Headteacher: Nicola Ware
DSL / safeguarding lead	Mr Andrew Growney
Deputy DSLs	Mrs Janet Spreadbury; Mrs Kirsty Whitlock
Computing / online safety lead	Louise Moore
Safeguarding governor	Eleanor Gash
Business / data systems lead	Denise McDonnell (confirm responsibilities locally)
Assessment period	September 2026 – July 2027
Review frequency	At least annually, termly in leadership review, and after a serious incident or significant change
Assessment status	Working draft for review and completion by school leaders, DSL, IT/filtering provider and governors

2. Purpose and scope

This assessment identifies foreseeable online safety risks to pupils, staff and the school community, and records controls, further actions and responsibility. It covers school-managed devices and networks, personal devices used on site, online platforms, digital communication, remote learning, data and accounts, and online activity that may affect pupils' welfare in school.

The assessment should be completed with the school's current Child Protection and Safeguarding Policy, Online Safety Policy, acceptable use agreements, behaviour and anti-bullying policies, data protection arrangements, mobile phone policy, and the school's filtering and monitoring procedures. It is not a substitute for those policies or for case-specific safeguarding action.

3. Risk rating method

Likelihood	Definition	Severity	Definition
1 – Unlikely	Not expected in normal circumstances	1 – Low	Limited impact; easily managed locally
2 – Possible	Could happen at some point	2 – Moderate	Meaningful impact; requires planned response
3 – Likely	Has happened or is reasonably foreseeable	3 – High	Serious harm, safeguarding or significant operational impact
4 – Very likely	Expected without strong controls	4 – Critical	Immediate danger, serious harm, major breach or sustained disruption

Risk score = likelihood × severity. Suggested bands: 1–3 Low; 4–6 Moderate; 8–9 High; 12–16 Critical. These ratings are initial planning judgements and must be validated against the school's actual systems, incidents and provider evidence. Residual risk should be reassessed after controls and actions are verified.

4. Online safety risk register

Risk / hazard	Potential harm	Initial risk	Current controls to verify	Further action required	Lead	When	Evidence
1. Harmful or age-inappropriate content	Pupils access pornography, violence, self-harm, hate, extremist or otherwise unsuitable content through school devices, web searches, apps or bypass methods.	3 × 4 = 12 Critical	Age-appropriate filtering; safe search locked where possible; managed accounts and devices; staff supervision; online safety curriculum; clear reporting route.	IT provider and Computing Lead to test filtering on representative devices and networks, including guest access and alternative browsers; record test date, results and fixes.	Computing Lead / IT provider; DSL informed of safeguarding concerns	Autumn 1; then termly and after changes	Testing log; filtering policy; curriculum plans; incident records
2. Filtering or monitoring failure	Filtering is disabled, misconfigured, over-blocks learning or does not cover devices, apps, off-site use or guest	3 × 4 = 12 Critical	Written filtering and monitoring arrangements; named responsible leads; provider support; reporting	Obtain written confirmation from IT/provider of what is filtered and monitored, coverage,	Headteacher / Computing Lead / IT provider / DSL	Autumn 1; termly checks	Provider statement; test records; alert logs; meeting minutes

	accounts. Alerts may not reach a responsible person.		and escalation process; review logs and alerts.	limitations, alert recipients, response times and service hours. Check at least annually and after significant change.			
3. Online bullying, harassment or harmful peer contact	Pupils are targeted through games, messaging, social media, group chats, images or anonymous accounts, including activity outside school that affects school life.	3 × 3 = 9 High	Anti-bullying and behaviour procedures; reporting routes; age-appropriate teaching; staff training; safeguarding recording; support for affected pupils.	Ensure staff know how to preserve relevant evidence safely, avoid circulating harmful images, record concerns and refer to DSL; reinforce parent/pupil reporting routes.	DSL / Deputy DSLs / Computing Lead / class teachers	Ongoing; review each incident	Safeguarding records; training records; pupil voice; policy review
4. Grooming, coercion, exploitation or unsafe contact	A pupil is contacted by an adult or peer who manipulates, threatens, requests images, seeks personal details or attempts to arrange an unsafe meeting.	2 × 4 = 8 High	Teaching about trusted adults, privacy, consent and reporting; filtering; supervised use; safeguarding response procedures; staff awareness.	Review curriculum coverage for grooming, coercion, image-based abuse and reporting; ensure all staff know to report immediately to DSL and follow child protection procedures.	DSL / Deputy DSLs / Computing Lead	Autumn 1 curriculum audit; termly review	Curriculum map; staff briefing; safeguarding records
5. Sharing of nude or sexual images / harmful images	Pupils create, receive, request or share indecent or sexual images, or encounter disturbing content.	2 × 4 = 8 High	Age-appropriate relationships and online safety education; clear reporting; staff follow current safeguarding guidance; do not view, download or forward images unnecessarily.	Brief staff on the current school response protocol, evidence handling and referral/escalation route. Ensure pupils know they can seek help without fear of blame.	DSL / Deputy DSLs	Autumn 1 and as guidance changes	Staff briefing; policy; incident records
6. Personal information, privacy and data protection	Children or staff disclose names, contact details, locations, images, sensitive information or school data to unauthorised people or platforms.	3 × 3 = 9 High	Approved platforms; privacy settings; permissions; staff training; data minimisation; secure storage and access controls; privacy notices.	Review platforms and apps used with pupils; check age requirements, privacy settings, data processing agreements and DPIAs where required. Remove unused accounts and review permissions.	Headteacher / data protection lead / IT provider	Autumn 1; before new tools; annually	Approved app list; DPIAs; privacy notices; account audit
7. Account compromise, phishing and cyber security	Weak passwords, phishing, malware, shared logins or insecure systems expose school data or disrupt teaching.	3 × 4 = 12 Critical	Unique accounts; strong authentication where available; secure configuration; updates; backups; access controls; phishing awareness; incident response arrangements.	Confirm multi-factor authentication for privileged/admin accounts where supported; review leavers' access, backups, patching and cyber incident response with IT provider.	Headteacher / Business Manager / IT provider	Autumn 1; termly access review	IT audit; backup checks; access review; incident plan
8. Unsafe use of AI and generative tools	Pupils or staff enter personal data into AI tools, generate harmful or misleading content, use deepfakes, or rely on inaccurate outputs.	3 × 3 = 9 High	Approved-use expectations; staff supervision; teaching on misinformation, privacy, copyright and respectful use; data protection controls.	Create/confirm a list of approved AI tools and prohibited uses; assess age limits and privacy terms; require staff to check outputs and never enter identifiable pupil or safeguarding information into unapproved tools.	Headteacher / Computing Lead / data protection lead	Autumn 1; before adopting a tool	Approved tool list; staff guidance; curriculum plans; DPIA if required
9. Staff conduct and professional boundaries	Staff communicate with pupils through personal accounts, share inappropriate content, use personal devices improperly or blur professional boundaries.	2 × 4 = 8 High	Staff code of conduct; acceptable use agreement; approved school communication channels; safeguarding training; whistleblowing and low-level concerns procedures.	Reissue annual acceptable use expectations; check staff know how to report a concern about an adult and how to manage accidental contact or inappropriate messages.	Headteacher / DSL	September 2026; annual refresh	Signed agreements; training log; policy review
10. Personal phones, smart watches and recording devices	Unauthorised recording, photographs, messaging or phone use causes privacy breaches, bullying or safeguarding concerns.	3 × 3 = 9 High	School mobile/smart technology policy; clear pupil/staff expectations; consent and image permissions; secure handling of school photographs.	Check school policy reflects statutory mobile phone guidance in force from September 2026; clarify exceptions, staff use, visitor expectations and response to breaches.	Headteacher / DSL / Computing Lead	Autumn 1; after incidents	Published policy; staff briefing; incident log
11. Online learning and third-party platforms	Pupils use unsafe links, public chat, unmoderated meetings or platforms that expose them to inappropriate	2 × 3 = 6 Moderate	Approved platforms; restricted access; teacher supervision; meeting controls; parent guidance; privacy and age checks.	Review any platform used for remote learning or pupil communication; disable unnecessary chat/recording; check access	Computing Lead / class teachers / IT provider	Before use and annually	Platform checklist; risk assessment; parent information

	contact or data collection.			controls and moderation arrangements.			
12. Digital inclusion and accessibility	Filtering or online safety measures block legitimate learning, or pupils with SEND/language needs cannot understand safety teaching or reporting routes.	3 × 2 = 6 Moderate	Staff review blocked resources; accessible teaching; alternative reporting methods; reasonable adjustments; inclusive curriculum.	Ensure online safety teaching and reporting are accessible to pupils with SEND and communication needs; provide an escalation route for over-blocking that affects learning.	SENCO / Computing Lead / class teachers	Termly curriculum review	Lesson plans; pupil voice; unblock logs
13. Harmful online challenges, self-harm or extremist content	Pupils encounter content encouraging dangerous challenges, self-harm, suicide, radicalisation or violence, or are drawn into harmful online communities.	2 × 4 = 8 High	Safeguarding curriculum; filtering; staff awareness; Prevent and child protection procedures; trusted reporting routes.	Check staff understand how online indicators are recorded and escalated to DSL; ensure any Prevent concerns follow school procedures and local referral arrangements.	DSL / Deputy DSLs / Computing Lead	Autumn 1; ongoing	Staff training; curriculum map; safeguarding records
14. Third-party provider or system outage	Filtering, monitoring, email, learning platforms or safeguarding systems fail, leaving pupils exposed or preventing timely response.	2 × 3 = 6 Moderate	IT support agreement; provider contacts; backup arrangements; incident reporting; manual supervision and fallback procedures.	Document what staff should do if filtering/monitoring is unavailable, including pausing unsupervised internet use and contacting IT/DSL. Test escalation contacts.	Business Manager / IT provider / DSL	Autumn 1; after outage	Business continuity plan; test log; provider SLA
15. Home use and online harm outside school	Online abuse, harmful content or contact occurs on personal devices or home networks and affects pupil welfare or school relationships.	3 × 3 = 9 High	Parent communications; pupil education; clear reporting routes; safeguarding response; signposting to support.	Publish parent guidance on reporting online harm, privacy settings, age-appropriate controls and how to share concerns with school. Make clear school will respond to safeguarding concerns affecting pupils.	DSL / Computing Lead / class teachers	At least once per term	Newsletters; parent resources; safeguarding records

5. Filtering and monitoring assurance checklist

- ☐ Named senior leader, DSL and technical lead responsibilities are recorded and understood.
- ☐ The school has written filtering and monitoring procedures and knows which devices, users, networks, apps and off-site use are covered.
- ☐ Safe search is enabled and locked where appropriate; pupils cannot easily bypass filtering through unauthorised browsers or plugins.
- ☐ Monitoring alerts are sent to named, trained staff and have a clear triage, recording and escalation route.
- ☐ IT/provider staff understand safeguarding escalation and report failures, suspicious activity and gaps promptly.
- ☐ The school checks that filtering and monitoring work at least annually, termly as part of local assurance, after serious incidents and after significant changes.
- ☐ Checks and tests are recorded, including date, device/location, user profile, outcome and action taken.
- ☐ Over-blocking is reviewed so that it does not unreasonably restrict teaching and learning.
- ☐ Monitoring access is restricted; data retention, privacy notices and any required DPIA are reviewed.
- ☐ The school has a clear process for what staff do if filtering or monitoring fails.

6. Incident response: minimum expectations

- Act promptly to protect the child or adult at risk. If there is immediate danger, follow emergency procedures.
- Report safeguarding concerns to the DSL or a Deputy DSL without delay; do not investigate independently or promise secrecy.
- Record the facts, actions and decisions using the school's approved safeguarding and incident recording systems.
- Preserve relevant evidence safely and proportionately. Do not forward, download or circulate illegal or harmful images; follow current safeguarding guidance and seek DSL advice.
- Contact the IT provider where a technical issue, account compromise, filtering failure or cyber incident is suspected.
- Escalate data breaches to the school's data protection lead and follow the school's breach reporting procedure.
- Review the incident afterwards and update risk controls, staff training or curriculum where needed.

7. Review schedule and action log

Due date	Action / assurance check	Owner	Completed / evidence	Further action / review date
September 2026	Confirm risk assessment, roles, policies and annual staff briefing.			
September–October 2026	Obtain written filtering and monitoring assurance from IT/provider; test coverage and escalation route.			
Autumn 2026	Review approved apps, AI use, mobile phone arrangements and data protection/privacy documentation.			
Each term	Review incidents, alerts, filtering tests, curriculum coverage and pupil/parent feedback.			
After a significant change or incident	Reassess relevant risks and record updated controls.			
July 2027	Complete annual review and agree priorities for 2027–2028.			

8. Approval

Role	Name	Signature / date
Headteacher	Nicola Ware	
Designated Safeguarding Lead	Andrew Growney	
Computing / online safety lead	Louise Moore	
Safeguarding governor	Eleanor Gash	

Guidance and reference links

Department for Education — Keeping Children Safe in Education 2026: https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

Department for Education — Filtering and monitoring: core standard: https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges/filtering-and-monitoring-core-standard

UK Safer Internet Centre — Appropriate monitoring: https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/appropriate-monitoring

UK Safer Internet Centre — Appropriate filtering: https://saferinternet.org.uk/guide-and-resource/teachers-and-school-staff/appropriate-filtering-and-monitoring/appropriate-filtering

Note: This is a school-specific working draft, not confirmation that any control is currently in place. The school should validate ratings and existing controls with its DSL, IT/filtering provider, data protection lead and governing body, and check against current statutory guidance and local procedures.