Banks Road Primary School
Prevent Risk Assessment

Prevent risk assessment for schools	
Person completing: James Savage	**Date Implemented:** 1st March 2026

Definitions (Statutory Prevent Terminology)

Term	Definition	Operational Use in School
Extremism	Vocal or active opposition to fundamental British Values (democracy, rule of law, individual liberty, mutual respect and tolerance of different faiths/beliefs). Includes calls for the death of members of the UK armed forces.	Used to frame risk assessment, staff training, decisions about visitors, and filtering/monitoring priorities.
Radicalisation	Process by which a person comes to support terrorism or extremist ideologies associated with terrorist groups; may occur online/offline and involve grooming, manipulation or exposure to extremist narratives.	Used in identification of indicators, early help, and referral thresholds.
Terrorism	Use or threat of action to influence government or intimidate the public for political, religious, racial or ideological cause; can include serious violence, property damage, endangering life, or serious risk to public health/safety.	Used to set filtering blocks, reporting pathways, and referral to Prevent/Channel.
Implementation note	These definitions are used consistently across safeguarding, curriculum and early-help processes so staff recognise indicators of extremist/radicalising risk.	Included in induction & refresher training; referenced in policies.

Prevent is one strand of the UK's CONTEST strategy; our practice aligns to Prevent's three objectives: tackling the ideological causes of terrorism, intervening early, and enabling disengagement/rehabilitation.

National Risks

What national risks are you aware of that could impact your area, setting, students or families? For example, online radicalisation			
Risk 1 **Online Radicalisation (dominant national risk)** The UK Government states that the terrorist threat today is dominated by individuals or small groups radicalised primarily online, often without direct contact with organised terrorist networks. Children and young people are especially exposed to: • extremist content on social media and gaming platforms, • self-radicalisation via algorithms, • anonymous online spaces (Discord, Telegram, Reddit-style forums), • conspiracy theory networks and mis/disinformation. This is the **most significant national risk for all schools**.	**Risk 2** **Extreme Right-Wing Extremism (ERWT)** The remainder of the UK's domestic terrorist threat is driven almost exclusively by Extreme Right-Wing Terrorism. National risks include: • anti-migration, anti-Muslim, racist narratives, • online hate ecosystems (e.g., Telegram channels), • conspiracy theories around demographic change, • youth recruitment into "meme-based" extremist subcultures. ERWT recruitment often intersects with misogyny, inceldom, anti-LGBTQ+ hate, and conspiracy content.	**Risk 3** **The Manosphere, misogynistic and incel-aligned radicalisation** National research highlights the growing risk of extremism-adjacent misogynistic networks influencing boys and young men. These movements can be gateways to broader extremist ideologies and violence. This affects schools via: • misogynistic online influencers, • forums normalising violence against women, • crossover into far-right and anti-democratic narratives. This is recognised as one of the fastest-growing radicalisation pathways in UK youth.	**Risk 4** **Mis/disinformation and conspiracy theories** The DfE confirms that schools must recognise conspiracy narratives as a national radicalisation risk. These may include: • anti-government/world-order conspiracies, • extremist reinterpretations of current events, • online echo-chambers fostering polarisation or hate. These risks often feed into ERWT, grievance-based or hybrid extremist views.

Local Risks

What specific local risks are you aware of that could impact your area, setting, students or families? E.g. local extremist activity (groups active in the area)			
Risk 1 **Online radicalisation affecting young people in Merseyside** Merseyside Police highlight that young people locally are highly vulnerable to online grooming, extremist influence and harmful content, often occurring rapidly and in hidden online spaces. This risk is increased by: • high local youth access to social media and gaming platforms, • exposure to extremist narratives through encrypted channels, • misinformation/disinformation affecting community tensions.	**Risk 2** **Extremist narratives exploiting local community tensions** While Liverpool has strong community cohesion, Merseyside Police recognise the need to address signs of hate, hostility or ideological influence early. Risks include: • far-right activity online targeting local minority groups, • anti-Muslim/anti-migration sentiment influenced by national rhetoric, • antisemitism and anti-LGBTQ+ hate surfacing on social platforms, • extremist exploitation of international conflicts to inflame local divides.	**Risk 3** **Emerging misogynistic/manosphere online harms affecting boys and young men** National extremism research shows that misogynistic content is a major gateway into extremism; Liverpool's Prevent partners have identified youth vulnerability to harmful online influencers and manosphere ideology. These risks align with Merseyside Police's statement that "radicalisation can take place very quickly" through online influence.	**Risk 4** **Youth-specific radicalisation risks (gaming platforms, Discord, TikTok, Telegram)** Merseyside Prevent teams state that online spaces frequented by young people are key locations for early radicalisation indicators. Local risks include: • extremist recruitment in gaming chats, • conspiracy-spreaders on TikTok influencing worldview, • unmoderated platforms (Telegram/Discord) used for hate content.

Leadership and Partnership

Category	Risk	Hazard	Risk Management (Controls)	RAG	Further Action Needed	Lead Officer	Date for Completion	Support Available
Leadership	School values/ethos do not promote resilience to extremism/British Values	Pupils, staff, governors at risk if values don't reflect tolerance/diversity/respect	Values set out; website display; values include tolerance, diversity, mutual respect			James Savage (DSL)		
Leadership	Leaders unaware of Prevent duty/contextual risks	Pupils/staff at risk	Leaders trained; keep up to date with local risks; DSL issues Prevent info; annual safeguarding audit; policy updated and online; Prevent info on website			James Savage (DSL)		
Leadership	Staff unaware of Prevent/British Values responsibilities	Pupils/staff at risk	All staff read CP Policy & KCSIE Pt 1; Prevent training (National College); HT attends DSL forum & CTLP briefings and disseminates; SMSC/assemblies promote British Values; diversity celebrated; Equality Policy & annual EDI; DSL/Prevent Lead aware of actions/referrals		Whole-staff competency assessment required.	James Savage (DSL)	April 2026	**Joanna Fitzsimmons** Prevent Education Officer **M**: 07515332702 **E:** joanna.fitzsimmons@liverpool.gov.uk
Leadership	Governors unable to monitor Prevent strategy	Pupils/staff at risk	All governors read CP Policy & KCSIE; link governor oversees Prevent			James Savage (DSL)		

Category	Risk	Hazard	Risk Management (Controls)	RAG	Further Action Needed	Lead Officer	Date for Completion	Support Available
Leadership	Staff do not support values/ethos or promote extremist ideas	Pupils/staff at risk	Recruitment reflects values & safeguarding; adverts include safeguarding; safer recruitment; Prevent questions at interview			James Savage (DSL)	April 2026	**Joanna Fitzsimmons** Prevent Education Officer **M**: 07515332702 **E:** joanna.fitzsimmons@liverpool.gov.uk
Partnership	Staff lack confidence to work with external agencies on extremism	Pupils/staff	Work with safeguarding partners; DSL knows escalation; CPOMS records			James Savage (DSL)		
Partnership	Visiting speakers expose pupils to extremist ideologies	Pupils	Materials checked pre-visit; visitors never left alone; rigorous checks; pastoral support; external leaflets checked by DSL			James Savage (DSL)		
Partnership	Staff unclear on standards when collaborating with external contributors	Pupils/staff	Governors read CP Policy & KCSIE; link governor monitors; leaders maintain LA/Prevent partner links			James Savage (DSL)		

Staff Conduct, Transferable Risk and Prevent (KCSIE 2025)

Aspect	Detail	School Response / Actions
Definition	Transferable risk: staff behaviour outside school indicating risk of harm to children or vulnerability to extremist ideology / harmful online behaviour.	Treat as safeguarding concern even if occurring off-site.
Examples	Sharing/endorsing extremist/hate content; participating in extremist groups/events/forums; misogynistic/racist/antisemitic/Islamophobic/homophobic views; conspiracy theories; activism crossing into extremist narratives; associations with those under investigation.	Report via concerns/allegations procedures; LADO consultation as appropriate. Where concerning behaviour does not meet the harm threshold, it is addressed under the Low-Level Concerns procedures in the Child Protection Policy, including conduct outside school which may indicate vulnerability to extremist influence or harmful online behaviour.
School response	1) Follow KCSIE procedures for staff concerns/allegations; 2) Consult LADO as needed; 3) Assess risk & Prevent implications; 4) Review professional duties/Teachers' Standards; 5) Proportionate action/supervision/referrals.	DSL leads; recorded on CPOMS; governance oversight.
Staff expectations	Uphold British Values; avoid normalising extremist/hate narratives; report concerns about colleagues; online anonymity ≠ reduced obligations; model respect/tolerance/lawful behaviour.	Included in code of conduct, induction & refreshers.

British Values and Prevent (Updated KCSIE 2025)

Aspect	Detail
Purpose	British Values are a core safeguarding mechanism and a key component of preventative education; embedded across curriculum, culture and decision-making to build resilience to extremist/harmful narratives.
Strengthened role	Zero-tolerance for misogyny/homophobia/racism/antisemitism/hate; challenge harmful online norms (extremist content, conspiracy, disinformation); support respectful relationships and critical thinking; prevent normalisation of abusive/extremist attitudes; encourage democratic participation (student voice).

Aspect	Detail
How BV supports Prevent	Recognise & challenge extremist/discriminatory narratives; understand online ideological manipulation; develop critical literacy; build confidence to report; underpin respect, equality, lawful behaviour.
Implementation	RSHE/PSHE/SMSC/Online Safety; curriculum mapping for debate/critical thinking; assemblies/theme weeks/pupil leadership; behaviour policy and whole-school messaging; staff modelling of inclusive behaviour.

Extremist Content Cross-Overs (Misogyny, Incel Ideology, Child Sexual Abuse (CSA)-Linked Extremism)

Aspect	Detail	Response
Key cross-over risks	Online misogyny; incel ideology; CSA-adjacent extremist content; hate-based ideologies (racism/antisemitism/Islamophobia/homophobia); conspiracy theories linking sexual harm & extremist narratives.	Treat as Prevent-relevant indicators; integrate into risk assessment and curriculum.
Why this matters	These harms can normalise hate/violence, escalate exploration, act as entry points to extremist communities, and increase vulnerability (isolation/identity conflict/exploitation).	Use Prevent pathways and early help.
School response	Include topics in online-safety, RSHE, PSHE; configure filtering/monitoring for flags; train staff to spot early signs; respond via Prevent & safeguarding; engage parents/carers as needed.	CPOMS recording; DSL oversight. Follow the Equality Policy (February 2026) for responding to misogyny, hate-based behaviour and prejudice-related incidents, including racism, homophobia, biphobia, transphobia, sexism and disablist behaviour.
Curriculum/pastoral	Teach respectful relationships/gender equality; safe discussion spaces; embed anti-discrimination & equality; targeted pastoral support for vulnerable pupils.	Annual review with Counter-Terrorism Local Profile (CTLP) updates.

Capabilities

Risk	Hazard	Risk Management (Controls)	RAG	Further Action	Lead Officer	Date for Completion	Support Available
Staff unaware of Prevent/British Values responsibilities	Pupils and staff	Staff read CP Policy & KCSIE Pt 1; online Prevent training; British Values taught via SMSC/assemblies; diversity celebrations; modelling respect; Equality Policy; DSL aware of Prevent responsibilities/referrals Staff follow the Data Protection Policy (April 2025) when handling Prevent-related digital information (including monitoring alerts, search logs and safeguarding records), ensuring GDPR-compliant secure storage, limited access and appropriate processing. Staff understand that pupils with SEND and additional needs may be at increased risk of grooming, exploitation, online harm or radicalisation, in line with the Child Protection Policy, and adapt monitoring, teaching and intervention accordingly.			James Savage (DSL)		
Governors cannot monitor Prevent effectively	Pupils and staff	All governors read CP Policy & KCSIE; link governor oversees Prevent compliance			James Savage (DSL)		
Staff do not support values/ethos or promote extremist ideas	Pupils and staff	Recruitment reflects values/safeguarding; values & safeguarding in adverts; safer recruitment; Prevent-specific interview questions			James Savage (DSL)		

Channel Process and Prevent Referrals (KCSIE 2025 Requirements)

Topic	Our Practice
Overview	Channel is a voluntary, confidential multi-agency process to safeguard those at risk of being drawn into terrorism. Prevent is safeguarding. All Prevent referrals are comprehensive, detailed and timely, using the National Prevent Referral Form.

Topic	Our Practice
DSL role	Understand local pathways; make timely referrals; work with Prevent teams/Merseyside Police/CSC; attend/contribute to panel; share info securely/proportionately; record all actions on CPOMS.
Indicators	Support for extremist ideologies; influence/grooming/recruitment; sharing/seeking extremist content; concerning views incl. hate/conspiracy; identified via monitoring/staff/peers/context. Contextual safeguarding notifications, including Operation Encompass and Missing-from-Home alerts, are recognised as vulnerability indicators and are considered alongside Prevent risk factors as required in the Child Protection Policy.
Procedure	1) DSL info-gathering → 2) Initial safeguarding assessment (incl. family/context) → 3) Consult Prevent/Merseyside Police → 4) Make referral (local/national form) → 5) Panel screening & vulnerability assessment → 6) Support plan (e.g., mentoring/MH/family/online-safety). In Merseyside we operate a 'double-door' entry: referrals are sent to the Police Prevent mailbox *and* to Children's Social Care (where appropriate). Police Prevent screen referrals prior to Channel Panel consideration. In line with the Child Protection Policy, Prevent concerns also follow Early Help and safeguarding thresholds where appropriate. All actions, including info-gathering, consultation, decisions and referrals, are recorded on CPOMS, and DSLs apply the same threshold guidance used for all safeguarding cases before escalating to Prevent/Channel. Referral route used: PREVENT@Merseyside.pnn.police.uk (with parallel safeguarding referral to Children's Social Care where indicated).
Consent	Channel is voluntary; parental consent usually required for children; refusal does not prevent other safeguarding action if risk remains.
Information sharing	Secure CPOMS storage; transfer key info within 5 days to new settings; records reflect decisions, actions, referrals, outcomes. Referral documentation: National Prevent Referral Form used, completed fully with detailed chronology, factors and vulnerabilities.
Post-referral monitoring	Continue wellbeing monitoring; update safeguarding plans; brief relevant staff proportionately; update Prevent RA if new risks emerge. Contextual safeguarding alerts, including Operation Encompass notifications and Missing-from-Home episodes, are reviewed as part of ongoing Prevent risk monitoring in line with the Child Protection Policy.

Information Sharing

Risk	Hazard	Risk Management (Controls)	RAG	Further Action	Lead Officer	Date for Completion	Support Available
Staff lack confidence to work with agencies / share concerns externally	Pupils and staff	Work with safeguarding partners; DSL knows contact/escalation routes; referrals recorded/followed up on CPOMS			James Savage (DSL)		
Staff unsure how to share/escalate Prevent concerns	Pupils and staff	Clear processes for raising & referring cases; DSL disseminates safeguarding updates; referral systems reviewed via pastoral/DSL channels			James Savage (DSL)		

Curriculum Mapping for Prevent, British Values and Online Safety

Strand	What pupils learn / how we deliver	Review / Impact
Core curriculum elements	British Values; online safety via **4Cs**; extremist narratives & conspiracy theories; critical/digital literacy; healthy relationships/respect/consent (RSHE); respect for difference/anti-bullying/anti-discrimination; how to report concerns.	Annual review; Counter-Terrorism Local Profile/local risk updates; national trends; KCSIE/RSHE updates; incidents inform updates. Curriculum reviews also incorporate the Equality Policy (Feb 2026), ensuring representation, challenge of stereotypes and development of identity-safe, inclusive classroom practice.
Subject contributions	RSHE/PSHE (respect, tolerance, grooming, influence); Computing/Online Safety (extremist content, algorithms, grooming, misinformation); SMSC (ethics, citizenship); History/RE (diversity, debate, beliefs); English (bias, persuasion, rhetoric).	Teacher CPD; scheme overviews; pupil voice; monitoring alerts trends.
Prevent-specific threads	Recognise symbols/narratives/tactics/online spaces; understand online/offline radicalisation; challenge stereotypes; value diversity; seek help; understand conspiracy harms.	Staff training & classroom guidance.
Staff training	Annual training on extremism/radicalisation; online risk pathways incl. disinformation/conspiracy; safe facilitation of sensitive discussions; escalation routes (Prevent/Channel).	Logs; evaluation; governance oversight.

Strand	What pupils learn / how we deliver	Review / Impact
Impact measures	Review safeguarding concerns linked to ideology/online; analyse SENSO/monitoring trends; pupil voice; RSHE/PSHE assessment.	Reported to SLT/governors.

Reducing Permissive Environments

Risk	Hazard	Risk Management (Controls)	RAG	Further Action	Lead Officer	Date for Completion	Support Available
Visiting speakers expose pupils to extremist ideologies	Pupils	Materials pre-approved; never left alone; rigorous checks; DSL pastoral support; external leaflets checked			James Savage (DSL)		
Curriculum fails to challenge extremism/promote British Values	Pupils	BV opportunities mapped; PSHE/RSE used for sensitive discussions			James Savage (DSL)		
Culture of inequality/abuse enables hate	Pupils/staff/governors/parents	Behaviour policy: no hateful behaviour; staff response to harassment; pupils challenge peers; strong SMSC & comms; robust pastoral (DSL/SENDCo/Pastoral Lead); strong multi-agency work. Prejudice-related incidents—including racism, misogyny, homophobia, biphobia, transphobia and disablist behaviour—are recorded, responded to and monitored in line with the Equality Policy (February 2026).			James Savage (DSL)		
British Values not promoted outside classroom	Pupils/staff	Democracy via school council/leadership elections; assemblies on diversity/human rights/respect; range of religious/cultural celebrations			James Savage (DSL)		

Online Safety Risk Framework (4Cs)

4C	Definition / Typical Risks	School Response / Controls
Content	Illegal/inappropriate/harmful content incl. extremist material; hate speech; conspiracy theories; misinformation/disinformation.	Filtering blocks; monitoring alerts; curriculum on critical literacy; staff training to spot indicators. Digital images, manipulated media and AI-generated deepfake content are addressed in line with the Online Safety Policy (Sept 2025), which sets out safeguarding requirements for creating, storing and sharing images, including protection against AI-altered or sexualised imagery. Staff and DSLs remain aware of proscribed organisations guidance when assessing content and concerns.
Contact	Harmful interactions incl. grooming/manipulation/recruitment via DMs, gaming, social, private groups.	Supervision & reporting; curriculum on safe contact; DSL referral routes.
Conduct	Pupil's own behaviour—sharing extremist content, joining harmful groups, normalising hate/violence.	Behaviour policy; curriculum on respectful conduct; proportionate sanctions & support; parent engagement.
Commerce	Scams; extremist fundraising; monetised platforms promoting harmful/ideological content.	Financial-scam education; parent comms; filtering keyword lists; staff vigilance.
How we use the 4Cs	Inform Prevent RA; shape filtering/monitoring; identify trends; plan curriculum; guide staff training; identify 3G/4G/5G risks beyond filtering.	Annual review; link to Channel thresholds where relevant.

Misinformation, Disinformation and Conspiracy Theories (Prevent Risk)

Type	Definition	School Response
Misinformation	False/misleading info shared without intent to harm; may normalise extremist ideas, stereotypes, confusion about events.	Digital literacy across curriculum; monitoring/filtering to detect linked terms; staff trained to spot influence; use early help when needed.

Type	Definition	School Response
Disinformation	Deliberately false info to cause harm/manipulate opinions; used by extremist groups (edited videos, fake news, manufactured “evidence”).	Critical literacy teaching; report/escalate via DSL; incorporate into Prevent training & alerts.
Conspiracy theories	Simplistic/harmful explanations blaming groups/institutions; often recruitment gateway.	Explicit teaching & discussion; pastoral intervention; parent engagement where proportionate.

Mobile Devices, Data Networks and Filtering Bypass Risk

Aspect	Details	Controls
Risk summary	Pupils can access unfiltered internet via 3G/4G/5G; exposure to extremist/illegal content outside school systems.	Clear on-site expectations; limit/prohibit use where appropriate; staff vigilance; curriculum education; DSL reporting route for personal device concerns; include in Prevent/Online Safety RAs.
Monitoring & intervention	School can’t filter personal data networks; staff monitor behaviour/context; CPOMS recording; inform parents/carers; early help where risks suggest vulnerability.	DSL oversight; connect to filtering & monitoring annual review. Searches of personal devices suspected to contain extremist or harmful content follow statutory Searching, Screening and Confiscation guidance, alongside the requirements of the ICT Acceptable Use Policy and the Child Protection Policy (including DSL involvement and legally compliant handling of digital material).
Prevent link	Mobile data is a high-priority Prevent risk factor; informs whole-school RA & filtering/monitoring review.	Documented in annual reviews & reports to governors.

Generative AI and Emerging Technologies (Prevent Risk)

Aspect	Detail	Controls / Teaching
Key risks	AI-generated extremist content; AI-driven mis/disinformation; deepfakes; algorithmic reinforcement; AI-assisted filter bypass; use of unmoderated AI platforms.	Include AI risks in annual filtering/monitoring review; configure blocks where possible; monitor AI-related searches/creation; staff vigilance for AI influence. All use of AI platforms must comply with the ICT and Internet Acceptable Use Policy (Nov 2025), which prohibits entering personal data into AI tools, restricts use to approved platforms only, and forbids undisclosed or unsafe AI-generated content.
Curriculum	Computing/Online Safety/PSHE/RSHE: recognise mis/disinfo & deepfakes; evaluate sources/algorithmic bias; understand extremist use of AI; safe/ethical AI use.	Teacher CPD; pupil resources; assessment of understanding.
Prevent alignment	AI harms treated as high-priority Prevent risk; included in risk assessments; concerns escalated to DSL; considered in referrals/early help; reflected in policies.	Annual review & governance oversight.

Filtering and Monitoring (Statutory Requirements – KCSIE 2025)

Theme	What we do	Evidence / Notes
Roles & responsibilities	DSL/Prevent Lead: reviews alerts, responds & refers; SLT: ensures compliance & oversees annual review; ICT Provider/Trust IT: technical configs, thresholds, tools, reporting; Governing Body: holds leaders to account.	Role descriptions; logs; reports.
Annual review	Formal annual review to meet DfE standards; reflect Prevent RA; address emerging threats (extremism, disinfo, conspiracy theories); include AI risks; balance safeguarding with learning access; use DfE *Plan Technology for Your School* tool.	Review minutes; action plan; governor reports.
Risk-based filtering	Block extremist/terrorist/radicalising content; monitor relevant search terms; apply extra restrictions for higher-risk groups (e.g., vulnerable/SEND/heavy users); consider 4Cs when reviewing levels.	Keyword lists; group policies; audit trail.

Theme	What we do	Evidence / Notes
Monitoring activity	Detect attempts to access extremist content; searches indicating ideological curiosity; interactions pointing to grooming/influence/recruitment; AI tool misuse to generate harmful content; DSL reviews alerts promptly.	SENSO/other logs; DSL actions; CPOMS. All filtering and monitoring logs, alerts and search records are processed and stored in accordance with the Data Protection Policy (April 2025), including GDPR-compliant secure storage, restricted access, encryption, and audit trail requirements.
Mobile data & personal devices	Recognise 3G/4G/5G bypass risk; control device use; educate pupils; include in Prevent considerations.	Policy & comms; staff briefings.
Generative AI	Regularly review AI risks; block/monitor AI-linked harms; address AI-amplified mis/disinformation and bypass attempts.	Filtering rules; training logs.

IT Policies

Risk	Hazard	Risk Management (Controls)	RAG	Further Action	Lead Officer	Date for Completion	Support
Pupils use school network/hardware to access extremist material	Pupils	Policies reference extremist risks; pupils report concerns; filtering in place; email monitoring; DSL reviews SENSO weekly; KCSIE 2025 training on filtering/monitoring (roles, annual review, 3G/4G/5G risks, AI risks, Prevent-informed decisions); Trust ICT monitoring; parent online-safety events; adopt updated AUA when issued. Processing of Prevent-related digital information (including SENSO alerts, monitoring logs and search-term reports) follows the Data Protection Policy (April 2025), ensuring GDPR-compliant secure storage, restricted access, encryption and appropriate handling.			James Savage (DSL)		

Risk	Hazard	Risk Management (Controls)	RAG	Further Action	Lead Officer	Date for Completion	Support
Pupils access extremist material on personal devices/social media or are targeted online	Pupils	ICT curriculum covers avoiding extremist content; parent guidance; website factsheets & weekly newsletters on online safety and counter-extremism.			James Savage (DSL)	April 2026	**Joanna Fitzsimmons** Prevent Education Officer **M**: 07515332702 **E:** joanna.fitzsimmons@liverpool.gov.uk
Filtering/monitoring levels set inappropriately	Pupils	Trust systems robust and tested; breaches reported to DSL/leaders for action.			James Savage (DSL)		

Visiting Speakers and External Organisations (Prevent & KCSIE 2025)

Stage	What we require	Notes / Evidence
Pre-visit vetting & risk assessment	Purpose/educational value; visitor background/organisation; online checks for extremist/controversial views; review all content/materials; consider remote/digital elements that could bypass filters; assess potential ideological influence.	Documented checklists; materials on file.
Supervision & delivery	Visitors never unsupervised with pupils; staff present throughout; active monitoring of content; immediate DSL report of concerns.	Visitor log; staff presence recorded.
Post-visit	Report concerns to DSL; record visitor/content/issues; update Prevent RA if new risks; consider parent comms if sensitive content discussed.	CPOMS entries; RA update log.
External orgs for online safety	Follow UKCIS guidance; ensure evidence-based & age-appropriate delivery; no promotion of unsafe tech/platforms; prevent exposure to extremist/harmful/commercial content.	Contracts/MoUs; QA notes.
Prohibited content/triggers	Political/ideological persuasion; promotion of extremist narratives; contradictions of British Values; attempts to gather pupil personal data or direct pupils to external platforms.	Stop session & DSL intervention.

Visitor-specific Risks Table

Risk	Hazard	Risk Management (Controls)	RAG	Further Action	Lead Officer	Date for Completion	Support
Exposure to extremist ideologies by visiting speakers	Pupils	Pre-approval of materials; never left alone; rigorous checks; proactive pastoral support; DSL/HT permission for leaflets			James Savage (DSL)		
Non-approved visitors access site to spread extremism	Pupils & staff	Sign-in with ID; accompanied on site; robust start/end-of-day arrangements with termly monitoring; colour-coded lanyards & challenge protocol; secure storage of hazardous substances; DSL/HT approves all external leaflets; thorough off-site trip risk assessment (EVOLVE).			James Savage (DSL)		