



Discovery Trust – School Online Safety Addendum 2026–27

Each Discovery Trust school must complete this addendum annually and whenever significant local arrangements change. The addendum records local implementation of the Trust-wide Online Safety Policy. It must not duplicate, amend or replace the substantive Trust policy.

School name	Captains Close Primary School
Headteacher / Principal	Natalie Willcock
DSL and Deputy DSLs	Liam Collins, Katie Calvert, Vikki Chapman, Kelly Bartram, Abbie Elphick, Jo Coombe DSL@dsatcaptainsclose.org
Nominated safeguarding link governor/advisory board member	eboulderson@dsatcaptainsclose.org
Local IT lead/contact	Msanderson@dsatcaptainsclose.org
External IT provider, if applicable	Senso

Filtering and monitoring

Filtering system/provider	Sophos firewall
Monitoring system/provider	Senso.cloud
Named senior leader responsible for filtering and monitoring standards	Natalie Willcock (Headteacher and DSL).
DSL involvement in filtering and monitoring	DSL oversees safeguarding implications of alerts, reviews trends and determines safeguarding actions.
Who receives filtering/monitoring alerts	DSL, Deputy DSLs and authorised ICT personnel as appropriate.
Who reviews alerts and how frequently	DSL team review safeguarding alerts daily during term time. High-risk alerts reviewed immediately. Senso team also alert the Headteacher and Assistant headteacher.
How safeguarding alerts are escalated locally	Urgent concerns reported immediately to DSL. Safeguarding actions recorded on CPOMS. Referrals made to external agencies where required.
How filtering and monitoring effectiveness is reviewed and recorded	Annual filtering and monitoring review completed using DfE Filtering and Monitoring Standards and recorded through safeguarding governance and online safety audit processes.
Date of most recent formal filtering and	September 2026 DSL

monitoring effectiveness review	
Participants in the review and governance oversight	Headteacher, DSL and Safeguarding Link Governor.
Frequency and location of operational filtering-check records	Reviewed termly and retained within senso online.
High-risk alert recipients, cover arrangements and routine monitoring review frequency	DSL first response. Deputy DSLs provide cover during absence. Daily review during term time.
Location of significant filtering, blocking, allowing or exception decision records	ICT records maintained by Discovery Schools Trust ICT Team with safeguarding oversight where applicable
Known limitations in filtering or monitoring coverage and mitigation	Personal devices used outside school cannot be monitored. Online safety curriculum, parental engagement and safeguarding education mitigate risk.
Date/signpost to relevant filtering or monitoring DPIA or privacy assessment, where applicable	

Devices and mobile technology

Local mobile phone arrangements	Pupils do not routinely use mobile phones during the school day. Phones brought to school must be handed to the school office and collected at the end of the day.
Smart watches and wearable technology	Wearable technology is banned for pupils (with medical exceptions based on risk assessment and approval in school). Wearable technology is not banned for staff but recording (including ambient/background recording) AI processing using the devices is.
Pupil-owned devices / BYOD	Not routinely permitted. Any exceptions authorised by school leaders.
School-owned devices and loan devices	Managed through Trust systems with filtering, monitoring and acceptable use expectations in place.
Post-16 or specialist provision arrangements, if applicable	N/A
Agreed exceptions for safeguarding, medical, SEND or other needs	Individual arrangements may be agreed by the Headteacher, DSL or SENDCo and recorded where necessary.

Communication, platforms and curriculum

Approved pupil communication platforms	Microsoft Teams (where used), school learning platforms and teacher-managed educational systems.
Approved parent/carers communication systems	Arbor, school email, school website, newsletters and approved messaging systems - dojo.
Online learning platforms	Microsoft 365, Teams, Office applications, skolon and approved curriculum resources - read write inc, TTRS, century.
Locally approved apps/services	Skolon used for approved apps.
Social media accounts operated by the	School Facebook account and any Trust-approved social

school	media platforms.
Locally approved AI tools or systems	Microsoft Copilot and approved Trust-authorized AI tools for educational and administrative purposes.
Online safety curriculum arrangements	Delivered through Computing, PSHE, assemblies, Crew discussions and Project Evolve resources.
Curriculum leads responsible	Computing Lead, PSHE Lead and DSL Team.
Date of most recent whole-colleague online safety update and induction arrangements	September 2026 safeguarding update and annual safeguarding induction
Role-specific training arrangements for DSL, filtering and monitoring lead and relevant IT colleagues	DSL refresher training, online safety training, filtering and monitoring updates and Trust safeguarding updates.
Routine parent/carers online safety communication and local reporting route	Website information, newsletters, safeguarding updates using social media and arbor.
Targeted parent/carers engagement relevant to current local risk, if applicable	Guidance shared regarding social media, gaming, online exploitation, AI tools and emerging online risks.
SEND/accessibility considerations	Visual supports, adapted teaching materials, communication aids and differentiated online safety education provided where required, including within The Nest ERB.

Reporting and local escalation

How pupils report online safety concerns	Any trusted adult, DSL team, teacher, Learning Support Assistant, ELSA, mentor, worry boxes and pupil voice systems.
How colleagues report safeguarding concerns	Immediate verbal report to a DSL where urgent, followed by CPOMS recording.
Local safeguarding recording system	CPOMS.
How parents/carers raise online safety concerns	Contact school office, class teacher, DSL team, Headteacher or email safeguarding concerns directly.
Local IT/cyber incident reporting route	Report immediately to ICT support and school leadership. Escalated to Trust ICT team where appropriate.
Compromised account / phishing / malware escalation route	Report immediately to ICT support and DSL if safeguarding implications exist. Trust IT procedures followed.
Escalation to Trust safeguarding, IT or data protection colleagues	Concerns escalated to Discovery Trust safeguarding, ICT and Data Protection Officer as required.

--	--

Local circumstances and review

Age range / phase considerations	Primary phase, ages 3-11 years.
SEND, specialist or alternative provision considerations	The Nest Enhanced Resource Base supports pupils with autism and complex communication needs. Online safety education is adapted where required.
Residential, post-16 or other specialist arrangements, if applicable	N/A
Identified local safeguarding risks relevant to online safety	Social media misuse, cyberbullying, gaming platforms, inappropriate content, online grooming, exploitation, live-streaming services, AI-generated content, image sharing and harmful online challenges.
Date addendum completed	27.9.2026
Date addendum reviewed	September 2027
Reviewed by	Natalie Willcock (Headteacher/DSL), Emma Boulderson (Safeguarding Link Governor), Discovery Schools Trust representative as appropriate.