



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	Redlands Community Primary
Headteacher / Principal	Michelle Rosenitsch
DSL and Deputy DSLs	Estelle Ewing, Michelle Rosenitsch, Hannah Oselton, Lindsey Ketteringham & Carla Fitzsimmons
Nominated safeguarding link governor/advisory board member	S Dalby
Local IT lead/contact	Discovery Schools IT
External IT provider, if applicable	N/a

Filtering and monitoring

Filtering system/provider	Securus
Monitoring system/provider	Securus
Named senior leader responsible for filtering and monitoring standards	Estelle Ewing, Deputy Headteacher and DSL
DSL involvement in filtering and monitoring	DSL oversees safeguarding implications, reviews concerns and ensures relevant alerts are recorded on CPOMS and escalated appropriately.
Who receives filtering/monitoring alerts	Headteacher and Deputy Headteacher/DSL
Who reviews alerts and how frequently	Headteacher and Deputy Headteacher review alerts promptly; high-risk alerts are reviewed without delay.
How safeguarding alerts are escalated locally	Escalate immediately to the DSL; record on CPOMS and refer to Trust safeguarding, police, CEOP, social care or other agencies where thresholds are met.
How filtering and monitoring effectiveness is reviewed and recorded	Annual formal review by the responsible senior leader, DSL and IT support, informed by Securus alerts, operational checks,

	safeguarding incidents, CPOMS trends, pupil voice and the SWGfL 360 Safe audit. Actions are recorded and reported through safeguarding assurance and governance.
Date of most recent formal filtering and monitoring effectiveness review	To be confirmed from the Trust annual review record.
Participants in the review and governance oversight	Headteacher, Estelle Ewing (DSL), Discovery Schools IT/Trust Online Safety Lead, with Advisory Board oversight by S Dalby.
Frequency and location of operational filtering-check records	Operational checks are completed and recorded for relevant devices and locations; exact frequency and record location to be confirmed with Trust IT.
High-risk alert recipients, cover arrangements and routine monitoring review frequency	Headteacher and Deputy Headteacher/DSL; deputy DSL cover applies during absence. High-risk alerts are escalated without delay.
Location of significant filtering, blocking, allowing or exception decision records	School/Trust filtering and monitoring review records and relevant IT service records.
Known limitations in filtering or monitoring coverage and mitigation	Personal devices, mobile data, hotspots, VPNs and home networks may sit outside school controls. Mitigation: school device rules, acceptable-use agreements, supervision, parent guidance, reporting routes and safeguarding/behaviour procedures.
Date/signpost to relevant filtering or monitoring DPIA or privacy assessment, where applicable	Confirm current Securus DPIA/privacy assessment with the Trust Data Protection Officer/IT team.

Devices and mobile technology

Local mobile phone arrangements	Pupil phones are not used during the school day. Where an older pupil brings a phone, it is handed to the classteacher before school and collected afterwards. Staff personal phones are used only during breaks/lunch and must not be used to photograph pupils or
---------------------------------	---

	contact pupils/parents.
Smart watches and wearable technology	Treated as personal electronic devices and not used during the school day unless an agreed exception applies.
Pupil-owned devices / BYOD	No general pupil BYOD..
School-owned devices and loan devices	School-owned and loan devices are used for schoolwork/homework under the pupil Acceptable Use Policy, with usernames/passwords kept secure, appropriate supervision and filtering/monitoring where technically possible. Damage or concerning content is reported to an adult.
Post-16 or specialist provision arrangements, if applicable	Not applicable - primary phase.
Agreed exceptions for safeguarding, medical, SEND or other needs	Individual exceptions may be agreed for safeguarding, medical or SEND needs following risk assessment and agreement with the Headteacher/DSL and parents/carers; arrangements are recorded and reviewed.

Communication, platforms and curriculum

Approved pupil communication platforms	TEAMS
Approved parent/carers communication systems	Email, telephone, school website/newsletters and Microsoft Teams year-group areas where appropriate.
Online learning platforms	TEAMS, Spelling Shed, TTRS
Locally approved apps/services	Microsoft 365/Teams, OneNote/Class Notebook, Reading Progress, Immersive Reader, Picture Dictionary, Spelling Shed, Times Tables Rock Stars, Project Evolve, Adobe Express, Minecraft Education and other Trust-approved Microsoft learning tools.
Social media accounts operated by the school	Facebook
Locally approved AI tools or systems	Trust-approved tools: Copilot Chat/Microsoft 365 Copilot (adults and pupils aged 13+), Reading Progress (Year 1+), Adobe Express (Year 1+) subject to Trust AI guidance.
Online safety curriculum arrangements	Project Evolve taught weekly in Years 1-6, with EYFS provision, a

	progressive long-term plan, half-termly assessment/evidence, assemblies and Safer Internet Day. Delivery is monitored through planning/Sways, learning walks, pupil voice and assessment analysis.
Curriculum leads responsible	Aabshar Piare/ Luke Garner, Computing and Online Safety Subject Lead, working with Estelle Ewing and SLT.
Date of most recent whole-colleague online safety update and induction arrangements	Online safety resources and staff/governor training evidence were submitted for the 360 Online Safety re-assessment on 21 May 2026. New colleagues receive policy, safeguarding, Acceptable Use and reporting expectations through induction.
Role-specific training arrangements for DSL, filtering and monitoring lead and relevant IT colleagues	The school Online Safety/DSL lead receives role-specific online safety training and liaises with the Trust Online Safety Lead; relevant IT colleagues provide technical support.
Routine parent/carers online safety communication and local reporting route	Online safety information is shared through curriculum activities, themed weeks, Safer Internet Day, assemblies, letters, newsletters, the school website, Discovery Live webinars, parent/carers meetings and secure Teams areas. Concerns can be raised with the class teacher, school office or DSL team.
Targeted parent/carers engagement relevant to current local risk, if applicable	Targeted guidance is shared in response to current risks, including messaging/group-chat concerns, harmful content, cyberbullying and safe use of devices at home. Additional support/signposting is provided to individual families where needed.
SEND/accessibility considerations	Teaching, controls and reporting routes are adapted to age, SEND, communication and vulnerability. Accessibility tools include Immersive Reader, Picture Dictionary, Reading Progress and OneNote; individual support and agreed device exceptions are risk assessed.

Reporting and local escalation

How pupils report online safety concerns	Tell a class teacher, key adult, ELSA or DSL. Pupils are explicitly taught to tell a trusted adult immediately if online content or contact worries, upsets or harms them.
How colleagues report safeguarding concerns	Report promptly to a DSL and record the concern on CPOMS in line with safeguarding procedures; urgent/immediate concerns are raised directly without delay.
Local safeguarding recording system	CPOMS
How parents/carers raise online safety concerns	Contact the class teacher, school office, Headteacher or DSL team by telephone, email or meeting. Concerns outside school that affect pupil welfare or safety are also reported through these routes.
Local IT/cyber incident reporting route	Report immediately to Discovery Schools IT; also notify the Headteacher/DSL where pupil, colleague or safeguarding risk may be present.
Compromised account / phishing / malware escalation route	Stop interaction, preserve evidence, change/reset credentials where advised and report immediately to Discovery Schools IT. Escalate to the Headteacher/DSL and Data Protection Officer where safeguarding or data risk is involved.
Escalation to Trust safeguarding, IT or data protection colleagues	The DSL/Headteacher escalates serious online-safety concerns to the Trust Head of Safeguarding; technical incidents to Trust IT; and actual or suspected data breaches/privacy concerns to the Trust Data Protection Officer, with statutory referrals where required.

Local circumstances and review

Age range / phase considerations	Primary phase, ages 4–11. Expectations, language, supervision and reporting routes are age appropriate, with simplified EYFS/KS1 Acceptable Use guidance and progressive
----------------------------------	--

	teaching through Years 1–6.
SEND, specialist or alternative provision considerations	Provision is adapted for SEND, anxiety, communication and emotional-regulation needs. Individual risk assessments, support plans, accessible tools and closer supervision are used where needed. Alternative provision currently includes The Hub Cic with named school oversight and at least half-termly review.
Residential, post-16 or other specialist arrangements, if applicable	No residential or post-16 provision. Educational residential trips use secure year-group Microsoft Teams areas for updates and photographs, accessible only to relevant pupils, parents/carers and staff.
Identified local safeguarding risks relevant to online safety	WhatsApp/group messaging and social-media trends affecting pupils; cyberbullying, harmful content/contact, image sharing, scams/phishing and attempts to bypass controls. Risks may be heightened by SEND, anxiety, emotional-regulation difficulties and family stress.
Date addendum completed	21 September 2026
Date addendum reviewed	21 September 2026
Reviewed by	Estelle Ewing and Michelle Rosenitsch, with Trust IT/Online Safety input as required