



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	Fossebrook Primary School
Headteacher / Principal	Sarah Evans
DSL and Deputy DSLs	DSL: Sancha Wallis – swallis@dsatfossebrook.org Deputy DSLs: Sarah Evans – sevens@dsatfossebrook.org Kara Cragg – kcragg@dsatfossebrook.org Rebecca Findlay – rfindlay@dsatfossebrook.org Abbie Hunt – ahunt@dsatfossebrook.org
Nominated safeguarding link governor/advisory board member	Sam Williams – swilliams@dsatfossebrook.org
Local IT lead/contact	Kate Lawson – klawson@dsatfossebrook.org
External IT provider, if applicable	Discovery Trust IT support itsupport@discoverytrust.org

Filtering and monitoring

Filtering system/provider	Sophos filtering, backed up by Wave9, managed through the Trust IT service.
Monitoring system/provider	Senso monitoring alerts, supplemented by classroom supervision and device-use expectations.
Named senior leader responsible for filtering and monitoring standards	Sarah Evans, Headteacher, supported by the DSL and Trust IT.
DSL involvement in filtering and monitoring	DSL, Sancha Wallis and Deputy DSLs Sarah Evans, Kara Cragg, Rebecca Findlay and Abbie Hunt review safeguarding-related filtering and monitoring concerns and ensure appropriate recording, action and escalation.
Who receives filtering/monitoring alerts	DSL team, Headteacher and nominated IT contact; Trust safeguarding/IT colleagues where required.
Who reviews alerts and how frequently	High-risk safeguarding alerts are reviewed promptly by the DSL team. Routine monitoring is reviewed at least weekly and more frequently where risk indicates.
How safeguarding alerts are escalated locally	Concerns are recorded on CPOMS and escalated to the DSL/Deputy DSL in line with safeguarding procedures.

	Where required, concerns are escalated to Trust safeguarding, IT, data protection colleagues or external agencies- where required, to children's social care, police or Trust safeguarding.
How filtering and monitoring effectiveness is reviewed and recorded	Effectiveness is reviewed termly through alert sampling, blocked/allowed request checks, pupil voice, staff feedback and the annual formal review.
Date of most recent formal filtering and monitoring effectiveness review	
Participants in the review and governance oversight	Headteacher, DSL, Deputy DSLs, local IT contact and nominated safeguarding link governor, Sam Williams, with Trust support where required.
Frequency and location of operational filtering-check records	Weekly operational checks are recorded in the school safeguarding folder and crossreferenced on CPOMS where pupil-specific concerns arise.
High-risk alert recipients, cover arrangements and routine monitoring review frequency	High-risk alerts: DSL team and Headteacher. Cover: Deputy DSLs Sarah Evans, Kara Cragg, Rebecca Findlay and Abbie Hunt. Routine monitoring review: at least weekly, with urgent escalation as needed.
Location of significant filtering, blocking, allowing or exception decision records	CPOMS for safeguarding decisions; local IT/admin records for technical allow/block/exception decisions. Exact shared location: To confirm.
Known limitations in filtering or monitoring coverage and mitigation	Personal mobile data and homeuse devices are not covered by school filtering. Mitigation includes supervision, acceptable use education, parent communication and prompt reporting routes.
Date/signpost to relevant filtering or monitoring DPIA or privacy assessment, where applicable	Trust DPIA/privacy assessment held centrally by the Data Protection Lead. School signpost: Trust Data Protection folder.

Devices and mobile technology

Local mobile phone arrangements	Pupils do not use mobile phones during the school day unless an agreed exception is in place. Devices brought to school are kept securely in line with local arrangements.
Smart watches and wearable technology	Smart watches and wearable devices with communication, camera or internet functionality are treated as mobile technology and managed in line with the mobile phone arrangements. Smart watches with camera, messaging or internet functionality are not worn by pupils during the school day unless agreed as part of an individual plan.
Pupil-owned devices / BYOD	No routine pupil BYOD. Any exceptional use must be agreed in advance, risk-assessed and supervised.
School-owned devices and loan devices	School-owned devices are managed through school/Trust systems and are asset tagged. They must be used in line with acceptable use, safeguarding and

	data protection expectations. Loan devices: are issued using the school loan agreement.
Post-16 or specialist provision arrangements, if applicable	Not applicable – primary phase provision.
Agreed exceptions for safeguarding, medical, SEND or other needs	Exceptions may be agreed for safeguarding, medical, SEND or accessibility needs following individual risk assessment and parent/carers agreement where appropriate.

Communication, platforms and curriculum

Approved pupil communication platforms	Microsoft 365 / Teams where approved and supervised; other pupil communication platforms: To confirm.
Approved parent/carers communication systems	ClassDojo, school office email/telephone, Arbor, newsletters and the school website.
Online learning platforms	Microsoft 365 / Teams and approved curriculum platforms. Full list: To confirm locally.
Locally approved apps/services	Microsoft 365, CPOMS, ClassDojo, SENSO and other Trust/school-approved services. Local app list: To confirm.
Social media accounts operated by the school	School social media accounts: Facebook and Instagram
Locally approved AI tools or systems	Microsoft Copilot / approved Microsoft 365 AI functionality where permitted by Trust guidance. No pupil use unless explicitly approved and risk-assessed.
Online safety curriculum arrangements	Online safety is taught through the computing curriculum, RSHE/personal development, assemblies and responsive safeguarding education.
Curriculum leads responsible	Computing/online safety lead: Kate Lawson PSHE/RSHE lead: Sancha Wallis
Date of most recent whole-colleague online safety update and induction arrangements	Annual safeguarding/online safety update at the start of the academic year; induction for new colleagues before or shortly after starting. Exact date: 1 st day of INSET (19.08.26)
Role-specific training arrangements for DSL, filtering and monitoring lead and relevant IT colleagues	The DSL, Deputy DSLs, filtering and monitoring lead and relevant IT colleagues complete role-specific training and Trust updates. Records retained locally/centrally as appropriate.
Routine parent/carers online safety communication and local reporting route	Parent/carers communication through ClassDojo, newsletters, website updates and direct contact with the school office/DSL team for concerns.
Targeted parent/carers engagement relevant to current local risk, if applicable	Provided in response to local safeguarding themes, pupil voice, parental feedback or emerging online risks. Current targeted focus: To confirm.
SEND/accessibility considerations	Reasonable adjustments and accessible approaches are considered for pupils with SEND, including explicit teaching, visual supports, repetition, individual risk assessment and liaison with families/professionals.

Reporting and local escalation

How pupils report online safety concerns	Pupils report concerns to a trusted adult, class teacher,
---	---

	DSL/Deputy DSL or through agreed pupil voice/safeguarding routes.
How colleagues report safeguarding concerns	Colleagues report safeguarding concerns immediately to the DSL, Sancha Wallis, or to Deputy DSLs Sarah Evans, Kara Cragg, Rebecca Findlay and Abbie Hunt, and record concerns on CPOMS.
Local safeguarding recording system	CPOMS
How parents/carers raise online safety concerns	Parents/carers raise concerns via the school office, ClassDojo, email/telephone or directly with the DSL, Deputy DSLs or Headteacher.
Local IT/cyber incident reporting route	Report immediately to the local IT contact/school office and Trust IT support. Safeguarding or data protection implications are escalated to DSL and Trust colleagues.
Compromised account / phishing / malware escalation route	Immediate escalation to Trust IT support and the Headteacher/DSL. Follow Trust cyber/data protection incident procedures, including password reset, account disabling and reporting where required.
Escalation to Trust safeguarding, IT or data protection colleagues	Escalate to Discovery Trust Head of Safeguarding, Trust IT and data protection colleagues as appropriate. Trust Head of Safeguarding: Zack Minton.

Local circumstances and review

Age range / phase considerations	Primary phase.
SEND, specialist or alternative provision considerations	Inclusive practice, SEND support and accessibility adjustments are considered within online safety education, monitoring and device-use arrangements.
Residential, post-16 or other specialist arrangements, if applicable	Not applicable.
Identified local safeguarding risks relevant to online safety	Online peer conflict, inappropriate content, social media and messaging outside school, AI-generated or altered content, cyberbullying, misinformation/disinformation and age-inappropriate gaming or app use.
Date addendum completed	31 August 2026
Date addendum reviewed	To be reviewed September 2027 / annually, or sooner if arrangements change.
Reviewed by	Sarah Evans, Headteacher; Sancha Wallis, DSL; Deputy DSLs Sarah Evans, Kara Cragg, Rebecca Findlay and Abbie Hunt; Sam Williams, nominated safeguarding link governor.