



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	Farndon Fields Primary School
Headteacher / Principal	Simone Harrison
DSL and Deputy DSLs	DSL: Simone Harrison DDSLs: Danielle Barton, Vicky Harrison, Terri Burningham, Pat Raxworthy (Preschool), Tracey Batson (Preschool)
Nominated safeguarding link governor/advisory board member	Verina Wenham
Local IT lead/contact	Jenn Wallis (Office manager) / Trust IT Service Desk
External IT provider, if applicable	n/a

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	Simone Harrison (Headteacher) supported by Safeguarding team
DSL involvement in filtering and monitoring	The DSL reviews high-risk safeguarding alerts, contributes to the annual effectiveness review and ensures online safety concerns are recorded on CPOMS.
Who receives filtering/monitoring alerts	Headteacher/DSL, Deputy Headteacher/DDSL and Trust IT Service Desk.
Who reviews alerts and how frequently	High risk alerts are reviewed on the same day. Routine monitoring reports are reviewed at least weekly by the DSL. Any actions are recorded on CPOMS.
How safeguarding alerts are escalated locally	Safeguarding alerts are triaged by the DSL. Immediate risk is escalated to children's social care, police or Trust safeguarding where required.

How filtering and monitoring effectiveness is reviewed and recorded	Effectiveness is reviewed termly through alert sampling, pupil voice, staff feedback and the annual safeguarding self-audit. Trust IT team have oversight of function and effectiveness of the filtering and monitoring platforms, including that the filters are functioning as expected and that devices are correctly allocated.
Date of most recent formal filtering and monitoring effectiveness review	June 2026 (Trust Safeguarding Audit)
Participants in the review and governance oversight	Headteacher, DSL, Trust Safeguarding Lead.
Frequency and location of operational filtering-check records	Weekly checks of routine SENCO alerts (as above), standing item on DSL agendas, half termly filters tests are carried out by the DSL and minuted, any concerns are escalated to Trust IT team. Pupil concerns are recorded on CPOMs.
High-risk alert recipients, cover arrangements and routine monitoring review frequency	High-risk alerts go to the DSL/Headteacher. Cover is provided by the Deputy DSL rota. Routine reports are reviewed weekly
Location of significant filtering, blocking, allowing or exception decision records	Maintained at a Trust level by IT team.
Known limitations in filtering or monitoring coverage and mitigation	Personal mobile data and homeuse devices are not covered by school filtering. Mitigation includes all pupil phones that require consent from parents / carers and are handed in at the start of the day, returned at home time with use inside the school fence line prohibited, 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 required as part of an individual health plan. Phones brought to school are switched off and stored securely by class teacher, all pupil phones require consent from parents / carers and are handed in at the start of the day, returned at home time with use inside the school fence line prohibited
Smart watches and wearable technology	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	BYOD is not permitted for pupils, except where formally agreed for SEND, medical or accessibility reasons.

School-owned devices and loan devices	School-owned devices are asset tagged, filtered, password protected and returned for checks when requested.
Post-16 or specialist provision arrangements, if applicable	Not applicable.
Agreed exceptions for safeguarding, medical, SEND or other needs	Any exception must be documented in the pupil's individual plan, agreed by the Headteacher/DSL and reviewed at least termly

Communication, platforms and curriculum

Approved pupil communication platforms	Microsoft Teams/Office 365 for Education where enabled and supervised; no direct messaging between staff and pupils.
Approved parent/carers communication systems	Arbor, school email, school website and official school social media channels.
Online learning platforms	Microsoft Teams, Microsoft 365, school-approved curriculum platforms and other Trust approved services
Locally approved apps/services	Apps/services are approved through the school leadership team and Trust processes before use, considering safeguarding, data protection and age appropriateness.
Social media accounts operated by the school	Official school Facebook/ Instagram accounts managed by authorised senior colleagues. No personal staff accounts are used for school communication.
Locally approved AI tools or systems	No pupil-facing generative AI tools are used without prior leadership, safeguarding and data protection approval. Staff may only use Trust-approved AI tools in line with policy. CoPilot (Staff only), TeachMate AI (Staff only), Adobe Express (staff and pupils)
Online safety curriculum arrangements	Online safety is taught through PSHE/RSE, computing, assemblies and responsive safeguarding work. Content includes the 4Cs, reporting concerns, misinformation, AI and respectful online behaviour.
Curriculum leads responsible	Computing Lead, PSHE/RSE Lead and Safeguarding team.
Date of most recent whole-colleague online safety update and induction arrangements	Whole school update 20 August 2026. Individual induction for new staff members
Role-specific training arrangements for DSL, filtering and monitoring lead and relevant IT colleagues	DSL, filtering and monitoring lead and IT colleagues complete role-specific training and updates through Trust safeguarding briefings and provider guidance.
Routine parent/carers online safety communication and local reporting route	Online safety messages are shared through newsletters, parent briefings and the school website. Concerns should be reported to the DSL via the school office, safeguarding email or website Green button.

Targeted parent/carer engagement relevant to current local risk, if applicable	Targeted communication is provided where local patterns emerge, for example online bullying, unsafe image sharing, gaming contact risks, social media behaviours or AI-generated content concerns
SEND/accessibility considerations	Teaching and reporting routes are adapted for pupils with SEND, communication needs or additional vulnerabilities. Individual plans and/or risk assessments are used where required

Reporting and local escalation

How pupils report online safety concerns	Pupils report to any trusted adult, through class worry boxes, Reflect check-ins, Green button or directly to the DSL team
How colleagues report safeguarding concerns	All colleagues report safeguarding concerns immediately to the DSL team and record the concern on CPOMS in line with the Trust Safeguarding and Child Protection Policy.
Local safeguarding recording system	All Discovery Trust schools use CPOMS as the local safeguarding recording system. Online safety concerns involving pupils are recorded on CPOMS in line with the Trust Safeguarding and Child Protection Policy.
How parents/carers raise online safety concerns	Parents and carers raise online safety concerns through the school office, safeguarding email address or directly with the DSL team. Urgent concerns are shared with the DSL the same working day and recorded on CPOMS where they relate to a pupil.
Local IT/cyber incident reporting route	Colleagues report IT or cyber concerns to the Headteacher and the Trust IT route. Where there is any safeguarding or pupil-related concern, the DSL is informed and the concern is recorded on CPOMS.
Compromised account / phishing / malware escalation route	Suspected phishing, malware, compromised accounts or suspicious emails are escalated through Tellatech and the Trust IT route. Where there is any safeguarding or pupil-related concern, the DSL is informed and the concern is recorded on CPOMS.
Escalation to Trust safeguarding, IT or data protection colleagues	The Headteacher/DSL escalates safeguarding implications to Trust safeguarding. Technical concerns are escalated through Discovery Trust IT/Tellatech. Any suspected personal data breach is reported to the Headteacher and escalated to the Trust Data Protection Lead in line with Trust data protection Procedures.

Local circumstances and review

Age range / phase considerations	Farndon Fields provides education from preschool and Reception to Year 6. Online safety teaching, supervision and reporting routes are adapted to pupils' age, development and communication needs. Early Years and younger pupils receive explicit, practical teaching through stories, modelling and adult-supported device use. Older pupils receive progressively more detailed teaching about social media, gaming, group chats, online contact, image sharing, misinformation, generative AI and how to seek help. Staff recognise that age restrictions do not prevent some primary-aged pupils from accessing services intended for older users, so teaching and safeguarding responses reflect pupils' actual experiences.
SEND, specialist or alternative provision considerations	n/a
Residential, post-16 or other specialist arrangements, if applicable	n/a
Identified local safeguarding risks relevant to online safety	Local risks are identified through CPOMS records, Senso alerts, behaviour and bullying records, pupil voice, parent/carers reports and staff observations. Areas for continued vigilance in Market Harborough include primary-aged pupils accessing age-restricted social media, messaging and live-streaming services; online bullying or conflict arising outside school and affecting pupils in school; unsafe contact, coercion or scams through gaming, group chats and shared-interest communities; sharing personal information, images, recordings or location data; exposure to harmful, sexualised, extremist or misleading content; misuse of generative AI, including fabricated or manipulated content; and attempts to bypass school controls using personal devices or mobile data. The DSL reviews patterns at least termly and after any significant incident, using findings to adapt curriculum content, parent/carers communication, staff briefings, supervision and individual risk management.
Date addendum completed	8 th September 2026
Date addendum reviewed	30 th September 2026
Reviewed by	Simone Harrison