



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.

Working draft note: Entries highlighted in pale yellow require local verification before approval. The remaining entries have been completed from current Merrydale records available to the author.

School name	Merrydale Junior School
Headteacher / Principal	Antony Corbett
DSL and Deputy DSLs	DSL: Antony Corbett. Deputy DSLs: Ben Arnell, Gemma Bryans, Kate Hodgkinson and Nikita Grant.
Nominated safeguarding link governor/advisory board member	Karen Ludden
Local IT lead/contact	Ben Arnell (school contact for IT support tickets); Discovery Trust IT Support Service Desk for technical support.
External IT provider, if applicable	Discovery Trust IT Support Service Desk / central IT service.

Filtering and monitoring

Filtering system/provider	Sophos XG provided by wave 9
Monitoring system/provider	Senso
Named senior leader responsible for filtering and monitoring standards	Antony Corbett, Headteacher and DSL, pending confirmation in the formal annual review.
DSL involvement in filtering and monitoring	The DSL provides safeguarding oversight, receives/escalates safeguarding concerns, and should participate in the formal effectiveness review.
Who receives filtering/monitoring alerts	Alerts are sent to the head teacher, Deputy headteacher
Who reviews alerts and how frequently	Alerts are reviewed immediately

How safeguarding alerts are escalated locally	Urgent or serious concerns are brought directly to the DSL or an available Deputy DSL and recorded on CPOMS. If the usual leads are absent, the designated lead for that period is communicated to colleagues.
How filtering and monitoring effectiveness is reviewed and recorded	Head of IT and service manager discuss what needs to be blocked or allowed. Shared locally and discussed with head teachers
Date of most recent formal filtering and monitoring effectiveness review	23.9.26 Completed by Kieron Webster
Participants in the review and governance oversight	Headteacher/DSL, Deputy DSL/IT contact, Trust IT representative and safeguarding link Advisory Board member.
Frequency and location of operational filtering-check records	N/A
High-risk alert recipients, cover arrangements and routine monitoring review frequency	Head teacher receives captures
Location of significant filtering, blocking, allowing or exception decision records	N/A
Known limitations in filtering or monitoring coverage and mitigation	In place, doesn't affect Merrydale as mainly for tablets, and children have them here. There is a Trust wide one
Date/signpost to relevant filtering or monitoring DPIA or privacy assessment, where applicable	N/A

Devices and mobile technology

Local mobile phone arrangements	Pupils are not expected to have access to mobile phones during the school day. Colleague phones must not be visible where children are present and must not be used to photograph pupils, including on trips and residential. Personal calls/messages are made only in areas closed to children. Exceptional access requires prior agreement from the Headteacher or Deputy Headteacher.
Smart watches and wearable technology	Treated consistently with pupil mobile devices: not used for communication, recording or internet access during the school day. Individual medical/SEND exceptions must be agreed and documented.

Pupil-owned devices / BYOD	No routine pupil BYOD. Any exceptional use must be authorised in advance, supervised and subject to school safeguarding, acceptable-use and filtering arrangements.
School-owned devices and loan devices	School-managed laptops/devices are used for teaching and learning. Staff laptops and any loan devices remain subject to Trust IT management, filtering/monitoring and acceptable-use expectations. Faults or losses are reported to the school IT contact/Trust IT Service Desk.
Post-16 or specialist provision arrangements, if applicable	Not applicable: Merrydale is a Key Stage 2 junior school.
Agreed exceptions for safeguarding, medical, SEND or other needs	Case-by-case exceptions may be agreed by the Headteacher/DSL with the SENDCo and parent/carer where necessary. The rationale, controls, duration and review date should be recorded.

Communication, platforms and curriculum

Approved pupil communication platforms	Microsoft 365 education accounts and teacher-managed Microsoft Teams/OneNote spaces, where used. Pupils do not use personal email, messaging or social-media accounts to communicate with colleagues.
Approved parent/carer communication systems	Arbor, ClassDojo, school email/telephone, the school website, ParentPay and School Grid, according to the purpose of the communication.
Online learning platforms	Microsoft Teams, OneNote, CENTURY, myON, Accelerated Reader and Times Tables Rock Stars (TTRS).
Locally approved apps/services	Microsoft 365, ClassDojo, ParentPay, School Grid, Arbor, CENTURY, myON, Accelerated Reader, TTRS, ScholarPack and CPOMS, subject to Trust approval and data-protection requirements.
Social media accounts operated by the school	School account identified in parent information: @MerrydaleJunior.

	X account
Locally approved AI tools or systems	Olex.AI pupil access is evidenced in school materials. Co-pilot for staff Adobe express has AI ability
Online safety curriculum arrangements	Online safety is taught through the Key Stage 2 curriculum, including password protection, cyberbullying, privacy and online monitoring/adult supervision. Teaching is reinforced through assemblies and wider safeguarding education. Year 6 also visits Warning Zone to learn about risk and risk management.
Curriculum leads responsible	Computing/online-safety curriculum lead: Leah Lawley, locally before approval. Safeguarding oversight: Antony Corbett (DSL).
Date of most recent whole-colleague online safety update and induction arrangements	Whole-colleague safeguarding INSET for 2026-27 is evidenced in the school training materials prepared on 24 th August 2026. New colleagues receive safeguarding induction and reporting expectations.
Role-specific training arrangements for DSL, filtering and monitoring lead and relevant IT colleagues	DSL and relevant leaders access Trust safeguarding/online-safety updates. Provider-specific filtering and monitoring training, dates and records
Routine parent/carers online safety communication and local reporting route	Information is shared through routine school communications, ClassDojo, email and the school website. Parents/carers raise concerns with the school office, class teacher or DSL; urgent safeguarding concerns are passed directly to a DSL.
Targeted parent/carers engagement relevant to current local risk, if applicable	Targeted advice/meetings are arranged where an individual pupil, cohort or emerging risk requires additional support.
SEND/accessibility considerations	Resources and reporting routes are adapted to pupils' communication, cognition, sensory and SEMH needs. Visual prompts, trusted adults, direct teaching, repetition and supported reporting are used as appropriate. Individual controls are agreed with the SENDCo and recorded.

Reporting and local escalation

How pupils report online safety concerns	Pupils can speak to a trusted adult, class teacher, pastoral colleague or DSL, and may also use class/school worry boxes. Concerns are taken seriously and followed up.
How colleagues report safeguarding concerns	Speak directly to a DSL for urgent/serious matters and make a record on CPOMS. If in doubt, colleagues seek out a DSL rather than relying only on an electronic entry.
Local safeguarding recording system	CPOMS.
How parents/carers raise online safety concerns	Contact the school office by telephone/email, speak to the class teacher, or request contact with the DSL/Deputy DSL. Immediate safeguarding issues are escalated to a DSL.
Local IT/cyber incident reporting route	Report to Ben Arnell/school leadership and raise a ticket with the Discovery Trust IT Support Service Desk. Where personal data may be affected, also notify the Trust data-protection route.
Compromised account / phishing / malware escalation route	Stop using the affected account/device, do not forward or interact with suspicious content, and report immediately to the Discovery Trust IT Support Service Desk and school leadership/DSL. Any possible personal-data breach is escalated to the Trust data-protection contact.
Escalation to Trust safeguarding, IT or data protection colleagues	Safeguarding matters escalate through the DSL to Discovery Trust safeguarding; technical/cyber matters to the Trust IT Support Service Desk; suspected personal-data breaches to the Trust data-protection contact. Named contacts and emergency cover

Local circumstances and review

Age range / phase considerations	Key Stage 2 junior school, Years 3 to 6, broadly ages 7 to 11. Teaching and controls are age-appropriate
----------------------------------	--

	and become progressively more sophisticated across the phase.
SEND, specialist or alternative provision considerations	Merrydale is inclusive and provides adapted support for pupils with SEND and SEMH needs. Online-safety teaching, communication and reporting routes are personalised where required, with SENDCo/DSL oversight.
Residential, post-16 or other specialist arrangements, if applicable	No post-16 or residential provision. For educational visits/residential trips, personal mobile phones must not be used to photograph pupils; school safeguarding and device arrangements continue to apply.
Identified local safeguarding risks relevant to online safety	Risks reflected in school evidence include weak password practice/account security, cyberbullying, privacy and inappropriate communication/content. The school also serves a high-EAL community, so communications should be accessible and checked for understanding.
Date addendum completed	3 September 2026 (working draft completed from available school records).
Date addendum reviewed	23.9.26
Reviewed by	Antony Corbett (Headteacher/DSL), with Trust IT and safeguarding link Advisory Board scrutiny to be confirmed.