



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	Mowmacre Hill Primary School
Headteacher / Principal	Isaac Howarth
DSL and Deputy DSLs	Ben Mooney (DSL) Donna Wilson (SENDCo) Rhea Sills Fiona Simmonds Julie Eyden Chris Brown Susan Edwards Barry Lamble Sandra Lloyd Dawn Breeze
Nominated safeguarding link governor/advisory board member	Rob Hinsley
Local IT lead/contact	Louise Curtis (School Business Manager) / IT Support Desk
External IT provider, if applicable	Trust-approved external IT support provider (where required)

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
Named senior leader responsible for filtering and monitoring standards	Headteacher, supported by DSL and Trust IT
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, DDSs and Trust IT Service Desk

Who reviews alerts and how frequently	Same working day. Routine monitoring reports are reviewed weekly by the DSL team
How safeguarding alerts are escalated locally	Safeguarding alerts are triaged by the DSL. Immediate risk is escalated to the headteacher and, where required, to children's social care, police or Trust Safeguarding Lead (Zack Minton)
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	15 September 2026
Participants in the review and governance oversight	Headteacher, DSL, Trust IT representative and safeguarding link governor. Summary reported through local governance arrangements.
Frequency and location of operational filtering-check records	Weekly operational checks are recorded in the school safeguarding folder and cross-referenced on CPOMS where pupil-specific concerns arise.
High-risk alert recipients, cover arrangements and routine monitoring review frequency	High-risk alerts go to the DSL, Deputy DSLs and Headteacher. Cover is provided by the Deputy DSL rota. Routine reports are reviewed weekly.
Location of significant filtering, blocking, allowing or exception decision records	Recorded in the filtering and monitoring review log, with pupil-specific safeguarding decisions also recorded on CPOMS.
Known limitations in filtering or monitoring coverage and mitigation	Personal mobile data and home-use 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.

Devices and mobile technology

Local mobile phone arrangements	Pupils do not use mobile phones during the school day. Phones brought to school are switched off and stored securely in the school office.
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. Loan devices are issued using the school loan agreement.
Post-16 or specialist provision arrangements, if applicable	Not applicable for this primary setting.
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 unsupervised 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/X account 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.
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	PSHE lead, Computing lead and DSL.
Date of most recent whole-colleague online safety update and induction arrangements	Whole-colleague update delivered September 2026. New starters receive

	online safety, acceptable use and filtering/monitoring information during induction.
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 or safeguarding email.
Targeted parent/carers 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 or AI-generated content concerns.
SEND/accessibility considerations	Teaching and reporting routes are adapted for pupils with SEND, communication needs or additional vulnerabilities. Individual 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, pastoral check-ins 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 school's local IT contact/School Business Manager and the Trust IT route, in line with local arrangements. 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 Trust IT/Tellatech. Any suspected personal data breach is escalated to the Trust Data Protection Lead in line with Trust data protection procedures.

Local circumstances and review

Age range / phase considerations	3-11
Residential, post-16 or other specialist arrangements, if applicable	N/A
Date addendum completed	01/09/26
Next review date	01/09/27
Reviewed by	Ben Mooney (DSL) 