



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	Leighfield Primary School
Headteacher / Principal	Sarah Eaton
DSL and Deputy DSLs	Sarah Eaton Steph Wallace Carissa Laird Alison Fogg
Nominated safeguarding link governor/advisory board member	Chris Bishop
Local IT lead/contact	itsupport@discoverytrust.org
External IT provider, if applicable	N/A

Filtering and monitoring

Filtering system/provider	SENSO
Monitoring system/provider	SENSO
Named senior leader responsible for filtering and monitoring standards	Sarah Eaton
DSL involvement in filtering and monitoring	Sarah Eaton
Who receives filtering/monitoring alerts	Headteacher and Deputy Headteacher
Who reviews alerts and how frequently	Weekly reports, or as relevant for any specific incidents.
How safeguarding alerts are escalated locally	Headteacher informed to investigate. Leighfield safeguarding processes are then following including appropriate recording and related actions as required.
How filtering and monitoring effectiveness is reviewed and recorded	Discovery Trust Safeguarding Audits and quality assurance monitoring.

Devices and mobile technology

Local mobile phone arrangements	Pupils in Years 5 and 6 who travel to and from school independently may bring a mobile phone to school with parental permission. Phones must be switched off on arrival and handed to the school office for secure storage throughout the school day. Mobile phones must not be used anywhere on the school site, including before-school clubs, breaktimes, lunchtimes or after-school activities. Any unauthorised use will be managed in line with the Behaviour Policy and Online Safety Policy. Staff personal mobile phones must not be used in the presence of pupils unless authorised for an educational or safeguarding purpose. School-issued devices or phones must be used for communication with parents and carers.
Smart watches and wearable technology	Pupils may wear basic fitness trackers or watches that tell the time. Smart watches with camera, internet access, messaging, social media, voice recording or calling functionality are not permitted during the school day unless agreed as part of an individual safeguarding, medical or SEND plan. Where a permitted smart watch is worn, it must be placed into "school mode" or equivalent settings that disable communication functions. Staff will challenge and restrict the use of any wearable device that presents a safeguarding concern.
Pupil-owned devices / BYOD	N/A
School-owned devices and loan devices	School-owned devices are managed in accordance with Discovery Trust safeguarding, filtering, monitoring, information security and data protection requirements. Devices are asset tagged, password protected and filtered through the school's approved filtering and monitoring systems.
Post-16 or specialist provision arrangements, if applicable	N/A
Agreed exceptions for safeguarding, medical, SEND or other needs	Exceptions may be agreed where the use of a personal device or wearable technology supports a pupil's medical condition, communication needs, SEND provision, safeguarding plan or accessibility requirements. Any exception must be documented within an individual risk assessment, pupil support plan or EHCP provision, approved by the Headteacher and DSL, communicated to relevant staff and reviewed at least termly

Communication, platforms and curriculum

Approved pupil communication platforms	Microsoft Teams and Microsoft 365 for Education are the school's approved pupil communication platforms where enabled and appropriately supervised. The direct messaging function is disabled for pupils. Any online
---	--

	communication between staff and pupils must take place through approved school platforms and for educational purposes only
Approved parent/carers communication systems	Arbor Parent Portal and Arbor messaging, school email, the Leighfield Primary School website, newsletters and official school social media channels are the approved methods of communication with parents and carers. Staff must not communicate with parents or carers through personal social media accounts or personal messaging services.
Online learning platforms	Microsoft 365, Microsoft Teams, Times Tables Rock Stars, Numbots, Adobe, Padlet and other Discovery Trust-approved educational platforms are used to support teaching and learning. Any new platform must be approved through the school's safeguarding, data protection and IT processes before implementation.
Locally approved apps/services	All apps and digital services used with pupils must be approved through Discovery Trust processes and reviewed for safeguarding, data protection and age appropriateness before implementation. Current approved services include Microsoft 365, Microsoft Teams, Times Tables Rock Stars, Numbots, Adobe Express, Microsoft Forms, Microsoft Sway, Purple Mash (where used), CPOMS and Arbor. Any new platform must be approved by school leaders, the DSL and Discovery Trust IT processes prior to use
Social media accounts operated by the school	Official Leighfield Primary School social media accounts on Facebook and Instagram are managed by authorised school leaders and used for parental communication, celebration of learning and community engagement. No personal staff social media accounts are used for school communications. Social media activity is managed in line with Discovery Trust policies and parental consent arrangements.
Locally approved AI tools or systems	Staff may use Trust-approved AI tools to support planning, administration, communication and resource creation in line with Discovery Trust Artificial Intelligence guidance. AI must not be used to make safeguarding decisions or process confidential pupil information without appropriate safeguards. Any pupil use of AI tools must be supervised, age-appropriate and approved through school safeguarding, curriculum and data protection processes.
Online safety curriculum arrangements	Online safety is delivered through the Computing curriculum – Project Evolve, PSHE/RSHE curriculum, assemblies, safeguarding workshops, themed events and responsive teaching linked to emerging risks. Learning

	includes online relationships, cyberbullying, privacy and security, misinformation, scams, online gaming, social media, digital footprints, image sharing, consent, AI, healthy screen use and reporting concerns. Pupil voice, local safeguarding intelligence and filtering and monitoring information inform curriculum content.
Curriculum leads responsible	Computing Lead, PSHE Lead and Designated Safeguarding Lead (Sarah Eaton) work collaboratively to oversee online safety education, curriculum progression and safeguarding responses.
Date of most recent whole-colleague online safety update and induction arrangements	Whole-colleague online safety update delivered during September 2026 safeguarding and statutory briefing. All new colleagues, volunteers and regular visitors receive online safety, filtering and monitoring, acceptable use and safeguarding information as part of their induction before working with pupils
Role-specific training arrangements for DSL, filtering and monitoring lead and relevant IT colleagues	The DSL, deputies and filtering and monitoring lead complete regular safeguarding and online safety training, including updates relating to filtering and monitoring standards, emerging risks, AI, cyber security and local safeguarding priorities. Relevant IT colleagues access specialist training and provider guidance relating to SENSO, cyber security, filtering and monitoring systems. Training records are maintained and reviewed through Discovery Trust safeguarding assurance processes.
Routine parent/carers online safety communication and local reporting route	Parents and carers receive regular online safety information through newsletters, the school website, Arbor communications, curriculum updates and safeguarding information. Online safety concerns can be reported via the school office, directly to the DSL team, or via email to dsl@dsatleighfield.org . Concerns relating to a pupil are recorded and managed in line with safeguarding procedures.
SEND/accessibility considerations	Online safety education is adapted to meet the needs of pupils with SEND and other vulnerabilities. Information may be presented using simplified language, visuals, repetition, structured teaching approaches and additional adult support where required. Individual risk assessments, SEND support plans and EHCP provision are considered when implementing online safety arrangements. Reporting routes are adapted to ensure all pupils can communicate concerns effectively.

Reporting and local escalation

How pupils report online safety concerns	Pupils are encouraged to report online safety concerns to any trusted adult in school. This may include their class teacher, teaching assistant, ELSA, Deputy DSL or DSL. Pupils may also raise concerns through worry boxes, pastoral check-ins, safeguarding lessons, assemblies or directly with a member of the safeguarding team. Pupils are regularly reminded that any online concern, whether occurring at school or outside school, should be shared with a trusted adult as soon as possible
How colleagues report safeguarding concerns	All colleagues must report online safety and safeguarding concerns immediately to the DSL or a Deputy DSL and record concerns on CPOMS in accordance with the Discovery Trust Safeguarding and Child Protection Policy. Concerns identified through direct disclosure, observation, filtering and monitoring systems or contact from parents/carers must be treated as safeguarding concerns and responded to without delay.
Local safeguarding recording system	Leighfield Primary School uses CPOMS as its safeguarding recording system. Online safety incidents, cyberbullying concerns, harmful online content, inappropriate communications, filtering and monitoring concerns and any related safeguarding actions are recorded on CPOMS in line with statutory guidance and Discovery Trust procedures.
How parents/carers raise online safety concerns	Parents and carers can raise online safety concerns through the school office, directly with the DSL team, by contacting the Headteacher, or via the safeguarding email address dsl@dsatleighfield.org . Concerns are assessed in line with the school's safeguarding procedures and recorded where appropriate.
Local IT/cyber incident reporting route	Suspected IT security incidents, inappropriate system use, data breaches, cyber security concerns or technical issues affecting pupil safety must be reported immediately to the Discovery Trust IT Support Service and the Headteacher. Where safeguarding implications are identified, the DSL will also be informed. All incidents are managed in accordance with Discovery Trust IT, safeguarding and data protection procedures.
Compromised account / phishing / malware escalation route	Any colleague who suspects a compromised account, phishing attempt, malware infection or other cyber security threat must report it immediately to Discovery Trust IT support via tellatech@discoverytrust.org and inform the Headteacher. Affected devices should not continue to be used until advice has been obtained. Where there is a risk to pupil data, safeguarding information or school systems, the incident will be

	escalated to relevant Trust safeguarding, IT and data protection colleagues.
--	--

Local circumstances and review

Age range / phase considerations	Primary
SEND, specialist or alternative provision considerations	N/A
Residential, post-16 or other specialist arrangements, if applicable	N/A
Date addendum completed	September 2026
Date addendum reviewed	
Reviewed by	