



# 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.

|                                                                   |                                                                                                                                                                           |
|-------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>School name</b>                                                | Badgerbrook Primary School                                                                                                                                                |
| <b>Headteacher / Principal</b>                                    | Jo Andrews                                                                                                                                                                |
| <b>DSL and Deputy DSLs</b>                                        | Jo Andrews and the school's trained deputy DSL team. Current named personnel are maintained on the safeguarding contacts poster and CPOMS; confirm names for publication. |
| <b>Nominated safeguarding link governor/advisory board member</b> | Badgerbrook Advisory Board safeguarding— Laura Bisiker                                                                                                                    |
| <b>Local IT lead/contact</b>                                      | School Office / designated school IT contact, with Trust IT support. Confirm named local lead.                                                                            |
| <b>External IT provider, if applicable</b>                        | Discovery Trust IT service and approved technical support provider — confirm current provider name.                                                                       |

## Filtering and monitoring

|                                                                               |                                                                                                                                                                                              |
|-------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Filtering system/provider</b>                                              | Trust-managed, cloud-based web filtering applied to school-network and managed-device access. Confirm current product/provider with Trust IT.                                                |
| <b>Monitoring system/provider</b>                                             | Trust-approved monitoring and alerting arrangements. Confirm current product/provider and scope with Trust IT.                                                                               |
| <b>Named senior leader responsible for filtering and monitoring standards</b> | Jo Andrews, Headteacher.                                                                                                                                                                     |
| <b>DSL involvement in filtering and monitoring</b>                            | The DSL contributes to the risk assessment, reviews safeguarding alerts, identifies emerging patterns and supports the annual effectiveness review alongside the Headteacher and IT support. |
| <b>Who receives filtering/monitoring alerts</b>                               | Designated safeguarding staff and authorised IT colleagues, according to alert severity and the Trust escalation protocol.                                                                   |
| <b>Who reviews alerts and how frequently</b>                                  | High-risk alerts are reviewed promptly on receipt. Routine alerts and trends are reviewed by the DSL team                                                                                    |

|                                                                                                       |                                                                                                                                                                                                                                                              |
|-------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                       | and relevant IT colleagues at least weekly and more often where risk indicates.                                                                                                                                                                              |
| <b>How safeguarding alerts are escalated locally</b>                                                  | Immediate referral to the DSL or deputy DSL; record on CPOMS; assess risk and take protective action. Escalate to Trust safeguarding, parents/carers, children's social care, police or CEOP as appropriate.                                                 |
| <b>How filtering and monitoring effectiveness is reviewed and recorded</b>                            | Annual formal review led by the Headteacher with the DSLs and IT support, informed by test checks, incident data, curriculum needs, blocked/allowed requests and stakeholder feedback. Outcomes and actions are recorded and reported to governance.         |
| <b>Date of most recent formal filtering and monitoring effectiveness review</b>                       | To be completed following the 2026–27 annual review.                                                                                                                                                                                                         |
| <b>Participants in the review and governance oversight</b>                                            | Headteacher, DSL/deputy DSL, local/Trust IT representative and safeguarding link advisory board member; assurance reported through the school and Trust governance arrangements.                                                                             |
| <b>Frequency and location of operational filtering-check records</b>                                  | Termly operational checks, and after significant system or curriculum changes, recorded in the school's secure safeguarding/IT compliance records.                                                                                                           |
| <b>High-risk alert recipients, cover arrangements and routine monitoring review frequency</b>         | DSL and deputies receive or are notified of high-risk alerts, with SLT cover during absence. Routine monitoring is reviewed at least weekly and trends are considered termly.                                                                                |
| <b>Location of significant filtering, blocking, allowing or exception decision records</b>            | Secure Trust IT service records and, where safeguarding is involved, CPOMS. Significant local decisions are retained with the annual review evidence.                                                                                                        |
| <b>Known limitations in filtering or monitoring coverage and mitigation</b>                           | Personal mobile data, unmanaged devices, encrypted services and home networks may fall outside school controls. Mitigation includes a phone-free school day, supervised use, acceptable-use agreements, education, reporting routes and parental engagement. |
| <b>Date/signpost to relevant filtering or monitoring DPIA or privacy assessment, where applicable</b> | Trust data-protection records — confirm current DPIA/privacy assessment reference and review date.                                                                                                                                                           |

## Devices and mobile technology

|                                              |                                                                                                                                                                                                                                         |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Local mobile phone arrangements</b>       | Badgerbrook is a mobile phone-free environment for pupils throughout the school day. Any phone brought for an agreed travel or safeguarding reason must be switched off, stored securely and not used on site without staff permission. |
| <b>Smart watches and wearable technology</b> | Devices capable of messaging, calling, recording, photographing or internet access must not be used during the school day. Where worn, communication and recording functions must be disabled; exceptions require prior agreement.      |
| <b>Pupil-owned devices / BYOD</b>            | Any BYOD are managed under the school filtering system. Personal devices may only be used where                                                                                                                                         |

|                                                                         |                                                                                                                                                                                                                                                               |
|-------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                         | explicitly authorised for an identified educational, safeguarding, medical or SEND purpose and subject to an individual risk assessment.                                                                                                                      |
| <b>School-owned devices and loan devices</b>                            | Managed school devices are configured with Trust controls, filtering and monitoring, named-user access and approved applications. Loan devices are issued under an agreement, must be returned promptly and any loss, damage or concern reported immediately. |
| <b>Post-16 or specialist provision arrangements, if applicable</b>      | Not applicable — primary provision.                                                                                                                                                                                                                           |
| <b>Agreed exceptions for safeguarding, medical, SEND or other needs</b> | Reasonable, documented exceptions may be agreed by the Headteacher/DSL with parents/carers and relevant professionals. Controls, supervision, review dates and safe-storage arrangements are recorded.                                                        |

## Communication, platforms and curriculum

|                                                     |                                                                                                                                                                                                                                                                             |
|-----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Approved pupil communication platforms</b>       | Trust-managed Microsoft 365 services and other curriculum platforms approved by the school/Trust. Pupil communication is supervised, age-appropriate and limited to school-managed accounts.                                                                                |
| <b>Approved parent/carer communication systems</b>  | Arbor communications, school email, telephone, letters/newsletters and the official school website. Urgent safeguarding matters should be reported directly to school rather than through social media.                                                                     |
| <b>Online learning platforms</b>                    | Trust-managed Microsoft 365 and school-approved curriculum resources, including ClickView and Vivi where deployed. Access is through managed accounts and age-appropriate controls.                                                                                         |
| <b>Locally approved apps/services</b>               | Only services approved through school/Trust procurement, data-protection and safeguarding checks may be used. Current registers are maintained by the school and Trust IT/data-protection teams.                                                                            |
| <b>Social media accounts operated by the school</b> | Official school accounts only, administered by authorised colleagues in line with the Trust policy, image consent and data-protection requirements. Confirm the current account list annually.                                                                              |
| <b>Locally approved AI tools or systems</b>         | Microsoft Copilot and any other Trust-approved AI tools may be used by authorised colleagues for appropriate professional purposes. Personal, special-category, safeguarding or identifiable pupil information must not be entered unless expressly approved and protected. |
| <b>Online safety curriculum arrangements</b>        | Taught progressively through computing and the wider PSHE/RSE curriculum, reinforced in assemblies, Safer Internet Day, digital-literacy work and responsive teaching following local incidents. Coverage addresses the 4Cs: content, contact, conduct and commerce.        |
| <b>Curriculum leads responsible</b>                 | Computing and PSHE/RSE leads, overseen by the Headteacher/DSL. Confirm current named leads.                                                                                                                                                                                 |

|                                                                                                              |                                                                                                                                                                                                                                 |
|--------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Date of most recent whole-colleague online safety update and induction arrangements</b>                   | Annual safeguarding and online-safety update at the start of the 2026–27 academic year; new colleagues receive this through induction. Record exact date in the training log.                                                   |
| <b>Role-specific training arrangements for DSL, filtering and monitoring lead and relevant IT colleagues</b> | Role-specific updates through Discovery Trust safeguarding/IT briefings, DSL continuing professional development and supplier guidance. Training is refreshed when systems, guidance or local risks change.                     |
| <b>Routine parent/carers online safety communication and local reporting route</b>                           | Advice is shared through newsletters, Arbor, the school website and targeted messages. Parents/carers report concerns to the school office, class teacher or DSL; urgent risks should be raised immediately.                    |
| <b>Targeted parent/carers engagement relevant to current local risk, if applicable</b>                       | Targeted reminders and resources on WhatsApp/social media, age restrictions, group-chat behaviour, image sharing, gaming, scams and device use are issued when incidents or emerging risks indicate.                            |
| <b>SEND/accessibility considerations</b>                                                                     | Teaching and reporting routes are adapted using explicit modelling, visual prompts, repetition, accessible formats and individual support. Risk assessments consider communication, cognition, sensory and vulnerability needs. |

## Reporting and local escalation

|                                                                           |                                                                                                                                                                                                                                                                           |
|---------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>How pupils report online safety concerns</b>                           | Pupils are encouraged to tell any trusted adult in school, their class teacher, a member of the safeguarding team or use any established pupil reporting/worry route. Reports are listened to, recorded and acted on promptly.                                            |
| <b>How colleagues report safeguarding concerns</b>                        | Report immediately to the DSL/deputy DSL and record on CPOMS in accordance with the Child Protection and Safeguarding Policy. Urgent concerns are communicated verbally without delay.                                                                                    |
| <b>Local safeguarding recording system</b>                                | CPOMS.                                                                                                                                                                                                                                                                    |
| <b>How parents/carers raise online safety concerns</b>                    | Contact the school office by telephone or email and ask to speak with the class teacher, Headteacher or DSL. Immediate danger should be reported to emergency services; concerns about online sexual abuse may also be reported to CEOP.                                  |
| <b>Local IT/cyber incident reporting route</b>                            | Report immediately to the designated school IT contact and Headteacher; log with the Discovery Trust IT service. Safeguarding or personal-data implications must also be referred to the DSL and Trust data-protection lead.                                              |
| <b>Compromised account / phishing / malware escalation route</b>          | Stop using the affected device/account, do not follow links or delete evidence, disconnect if advised, and contact Trust IT immediately. Notify the Headteacher and data-protection/safeguarding leads where relevant; reset credentials only through approved processes. |
| <b>Escalation to Trust safeguarding, IT or data protection colleagues</b> | The Headteacher/DSL escalates significant safeguarding matters to the Trust Head of Safeguarding, technical                                                                                                                                                               |

|  |                                                                                                                                                                        |
|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | incidents to Trust IT, and suspected personal-data breaches to the Trust data-protection lead, following Trust incident procedures and statutory reporting timescales. |
|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Local circumstances and review

|                                                                             |                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Age range / phase considerations</b>                                     | Primary provision from EYFS to Year 6. Teaching, supervision and access controls are developmentally appropriate, with greater adult guidance for younger pupils and increasing emphasis on critical thinking, privacy, consent and responsible independence in Key Stage 2.                                              |
| <b>SEND, specialist or alternative provision considerations</b>             | Individual vulnerabilities are considered through safeguarding and SEND planning. Adjustments may include simplified language, visual supports, close supervision, restricted functionality, social stories and personalised reporting routes.                                                                            |
| <b>Residential, post-16 or other specialist arrangements, if applicable</b> | Not applicable.                                                                                                                                                                                                                                                                                                           |
| <b>Identified local safeguarding risks relevant to online safety</b>        | Age-inappropriate social media and messaging, including WhatsApp group chats; cyberbullying and peer conflict; image sharing; gaming and contact with unknown users; misinformation; online scams; excessive use and digital wellbeing; and the use of unmanaged personal devices or mobile data outside school controls. |
| <b>Date addendum completed</b>                                              | 3 September 2026.                                                                                                                                                                                                                                                                                                         |
| <b>Date addendum reviewed</b>                                               | To be reviewed by September 2027, or sooner following significant change or incident.                                                                                                                                                                                                                                     |
| <b>Reviewed by</b>                                                          | Jo Andrews, Headteacher; DSL team; Trust IT/safeguarding representative; and safeguarding link advisory board member.                                                                                                                                                                                                     |