Trust-wide Online Safety Policy 2026–2027

One central policy for all Discovery Trust schools, supported by a short School Online Safety Addendum.

Version number	5.0
Consultation groups	Central Executive Team, Blended learning network, IT technicians and Headteachers
Approved by	Board of Trustees
Approval date	September 2026
Adopted by	Advisory Board
Adopted date	September 2026
Policy/document owner	Trust Head of Safeguarding
Status	Mandatory Trust policy – implementing statutory safeguarding duties and guidance
Frequency of review	Annual
Next review date	September 2027
Applicable to	All Discovery Trust schools and relevant Trust settings

Document History

Version	Version Date	Author	Summary of Changes

V1.0	9th September 2021	Adam Lapidge – Online Safety Lead	*New policy prepared in line with:* • *Keeping Children Safe in Education – September 2021* • *Working Together to Safeguard Children, 2018* • *Ofsted's Review of Sexual Abuse in Schools and Colleges – June 2021*
V2.0	6th September 2023	Adam Lapidge – Online Safety Lead	*Updated policy in line with:* • *Keeping Children Safe in Education – September 2023* • *DfE Filtering and Monitoring Standards*
V3.0	16th August 2024	Adam Lapidge – Online Safety Lead	*Updated policy:* • *Updated wording for curriculum to fit all schools.* • *Updated annex 1: Technical Systems* • *Updated linked policies to include AI* • *AI subsection added*
V4.0	29th August 2025	Adam Lapidge – Online Safety Lead	*Updated policy:* • *Removed 'staff' and replaced with 'colleague' throughout document.* • *Updated section on mobile devices* • *Updated section on AI* • *Updated section on Pupil smart watches* • *Added section on Digital Wellbeing*
V5.0	September 2026	Zack Minton – Head of Safeguarding / Jo Stone – Pedtech Lead	Full Trust-wide restructure for 2026–27. Reframed online safety as a core safeguarding responsibility; strengthened governance, filtering and monitoring, DSL involvement, IT assurance, AI and emerging technology, harmful online activity, devices, communication, remote learning, reporting, recording and escalation. Replaced local policy rewriting with a standard School Online Safety Addendum and added a final assurance check for governance review. September 2026 final strengthening pass added further precision on filtering and monitoring effectiveness, mobile phones, training assurance, parent/carer engagement, data protection safeguards and addendum evidence fields.

Contents

Discovery Trust Online Safety Policy 2026–27 1

1. Policy statement 1

2. Scope 1

3. Linked policies and procedures 3

4. Roles, responsibilities and governance 3

4.1 Governance 4

4.2 Trust Online Safety Lead / Trust safeguarding leadership 5

4.3 Headteachers / Principals and senior leaders 6

4.4 School Online Safety Lead / Designated Safeguarding Lead responsibilities 7

4.5 School IT colleagues, Trust IT colleagues and external IT providers 8

4.6 Teaching and support colleagues 9

4.7 Pupils 10

4.8 Parents/carers 11

4.9 Community users 12

5. Filtering and monitoring 13

5.1 Governance and accountability 13

5.2 Minimum expectations 13

5.3 Operational checks, review and evidence 14

5.4 Data protection and monitoring 15

5.5 Responding to alerts and concerns 15

5.6 Local information 15

6. Online safety in the curriculum 16

6.1 Curriculum expectations 16

6.2 Age, stage and vulnerability 16

6.3 Artificial intelligence, synthetic media and emerging technology 17

6.4 Local curriculum recording and assurance 18

7. Artificial intelligence and emerging technology 18

7.1 Core expectations 18
7.2 Safeguarding risks 19
7.3 Colleague use of AI 19
7.4 Pupil use of AI 19
7.5 Approval, review and local recording 20
8. Harmful online activity and safeguarding escalation 20
8.1 Types of harmful online activity 20
8.2 Safeguarding escalation 21
8.3 Recording, evidence and pupil support 21
9. Devices and acceptable use 22
9.1 Acceptable use 23
9.2 Trust-owned and school-owned devices 23
9.3 Personal devices, mobile phones and smart technology 24
9.4 Cameras, images, recordings and livestreaming 24
9.5 Searching, confiscation and examination of devices 24
10. Communication and social media 25
10.1 Professional boundaries and approved communication 25
10.2 Social media 25
10.3 Messaging, video conferencing, livestreaming and online learning 26
10.4 Communication with parents and carers 26
11. Remote learning 27
12. Policy review and assurance 27
12.1 Trust assurance 28
12.2 School assurance 28
12.3 Improvement and escalation 29
Discovery Trust – School Online Safety Addendum 2026–27 ..... Error! Bookmark not defined.

Filtering and monitoring.....Error! Bookmark not defined.

Devices and mobile technology .....Error! Bookmark not defined.

Communication, platforms and curriculum .....Error! Bookmark not defined.

Reporting and local escalation.....Error! Bookmark not defined.

Local circumstances and review.....Error! Bookmark not defined.

Discovery Trust Online Safety Policy 2026–27

This policy applies from 1 September 2026 to all Discovery Trust schools and relevant Trust settings. It is a single Trust-wide policy approved by the Discovery Trust Board of Trustees. Schools must not rewrite, amend or replace the core policy. Each school must complete the Discovery Trust – School Online Safety Addendum to record local implementation arrangements only.

Policy hierarchy: This Trust Online Safety Policy sets the mandatory safeguarding principles, minimum standards, governance arrangements, responsibilities and expectations that apply across every Discovery Trust school. Each school must maintain a short School Online Safety Addendum which records how these requirements are implemented locally. Detailed technical instructions, system configuration notes, IT processes and day-to-day classroom procedures must sit in operational procedures rather than in the published Trust policy or school addendum.
Schools must not edit the wording of the substantive Trust policy. Where local variation is required because of phase, provision, pupil need, local staffing, local systems or site-specific arrangements, schools must record this in their School Online Safety Addendum. The Trust policy and the completed school addendum should be read together.

1. Policy statement

Discovery Trust recognises online safety as an integral part of safeguarding and pupil welfare. It is not a separate IT issue. Pupils' learning, relationships, communication, identity, behaviour and wellbeing are increasingly shaped by digital technology, including social media, messaging, gaming, livestreaming, artificial intelligence, connected devices and online services. The Trust therefore expects online safety to be understood, led and reviewed as part of everyday safeguarding practice. Online safeguarding concerns must be identified, reported, recorded and responded to through the same safeguarding culture and procedures that apply to concerns arising offline. Where online activity indicates risk of harm, vulnerability, abuse, exploitation, harassment, discrimination, radicalisation, sexualised behaviour, cyber security concern, data protection concern or adult conduct concern, colleagues must follow the relevant safeguarding, conduct, cyber security or data protection route without delay.
The Trust's approach follows a clear safeguarding golden thread: national legislation and guidance inform Trust governance; Trust governance sets policy, minimum expectations and assurance arrangements; schools implement those expectations through leadership, DSL oversight, curriculum, technical controls and colleague practice; concerns are identified, reported, recorded and escalated; implementation is tested through review and quality assurance; and strategic assurance is reported to Trustees. Local operational information must be recorded in each school's Online Safety Addendum rather than by changing this Trust-wide policy.

2. Scope

This policy applies to online safety across all Discovery Trust schools, settings, activities, systems and digital environments. It covers safeguarding risks and responsibilities arising from the use of technology in school, at home, during remote or blended learning, on school visits, during Trust or

school activities, and where online behaviour outside school affects, or may affect, the safety, wellbeing, education, conduct or reputation of pupils, colleagues, schools or the Trust.

- This policy applies to trustees, Trust leaders, headteachers, Designated Safeguarding Leads, Deputy DSLs, governors/advisory board members, teaching colleagues, support colleagues, central colleagues, IT colleagues, external IT providers, volunteers, contractors, visitors, community users, pupils, parents and carers where they access, use, manage or are affected by Trust or school systems, devices, networks, digital platforms or communication systems.
- It applies to Trust-owned and school-owned devices, networks, accounts, platforms, filtering and monitoring systems, cloud services, email, collaboration tools, online learning platforms, communication systems, cameras, recording equipment, mobile technology, wearable technology, approved applications and approved AI tools.
- It also applies where personal devices, personal accounts, mobile data, hotspots, social media, messaging services, gaming platforms, livestreaming, artificial intelligence tools or other online services create a safeguarding, behaviour, professional conduct, cyber security, data protection or reputational concern connected to the Trust or one of its schools.

The policy should be read alongside the Discovery Trust Safeguarding and Child Protection Policy, Ready to Learn Policy, Anti-Bullying Policy, Data Protection and Information Security arrangements, Acceptable Use agreements, colleague conduct expectations, mobile-phone and smart-technology arrangements, communication expectations and relevant local procedures.

Schools must use this policy to establish consistent safeguarding expectations while recording schoolspecific implementation in the School Online Safety Addendum. The addendum must capture local information such as named leads, filtering and monitoring providers, operational checks, local device arrangements, approved platforms, approved AI tools, reporting routes, curriculum delivery and relevant school-specific circumstances.

Discovery Trust's approach to online safety is informed by four recognised categories of online risk:

Content risk: being exposed to illegal, inappropriate or harmful content such as pornography, misinformation, disinformation, fake news, conspiracy theories, racism, misogyny, self-harm content, suicide content, radicalisation, extremism and content generated or manipulated by artificial intelligence.

Contact risk: being subjected to harmful online interaction with peers, adults or organisations, including grooming, child sexual exploitation, criminal exploitation, coercion, financial exploitation, inappropriate commercial contact, and adults or AI-enabled systems posing as children or trusted individuals.

Conduct risk: personal online behaviour that increases the likelihood of, or causes, harm. This includes cyberbullying, sharing nudes and semi-nudes, online harassment, abusive communications, misogynistic content, misuse of artificial intelligence tools, harmful sexual behaviour and behaviours that place pupils or others at risk.

Commerce risk: risks such as online gambling, phishing, scams, fraud, inappropriate advertising, financial exploitation, extortion, sextortion and attempts to obtain personal information for criminal purposes.

These categories are not exhaustive. Schools must remain alert to emerging risks, including risks linked to artificial intelligence, synthetic media, online influence, financially motivated harm, harmful online communities and new technology used by pupils or adults. Online safety must therefore be addressed through safeguarding practice, curriculum, colleague training, technical controls, pupil voice, parental engagement, local recording and Trust assurance.

3. Linked policies and procedures

This policy should be read alongside the following Trust policies, procedures, guidance and local implementation records. Together, these documents provide the safeguarding, behaviour, conduct, data protection, information security, curriculum and operational framework within which online safety is implemented.

- Safeguarding and Child Protection Policy
- Ready to Learn Policy
- Anti-Bullying Policy, including cyberbullying arrangements
- Child-on-child abuse procedures and related safeguarding guidance
- Managing allegations, low-level concerns and colleague conduct procedures
- Relationships, Sex and Health Education Policy and curriculum documentation
- SEND Policy and accessibility arrangements
- Data Protection Policy, privacy notices, records management and information governance procedures
- Information Security and Cyber Security arrangements
- Acceptable Use agreements for pupils, colleagues, governors, volunteers, contractors, visitors and community users
- Filtering and monitoring procedures, review records and local assurance evidence
- Mobile phone, smart technology, wearable technology and personal device arrangements
- Searching, screening and confiscation procedures
- Code of Conduct and professional boundaries guidance for colleagues
- Social Media Policy and approved communication expectations
- Remote learning, online learning and platform-use protocols
- AI governance guidance, approved tool arrangements and local records of authorised AI use
- Whistleblowing and complaints procedures
- School Online Safety Addendum and any referenced local operational procedures

The above list is not exhaustive. Schools must not create separate local versions of this Trust policy. Where practice varies locally, the mandatory Trust expectation must remain in this policy and the school-specific implementation detail must be recorded in the School Online Safety Addendum or in a clearly referenced local operational procedure. Local operational records should be proportionate, current and capable of demonstrating how the Trust standard is implemented in practice.

4. Roles, responsibilities and governance

Discovery Trust takes a whole-Trust approach to online safety. Online safety is a core safeguarding responsibility and must be embedded in governance, executive leadership, school leadership, DSL

practice, curriculum, behaviour, pastoral support, technical systems, colleague conduct, pupil voice and parental engagement. Responsibilities must be explicit so that leaders can demonstrate who does what, how implementation is checked, and how concerns or weaknesses are escalated.

4.1 Governance

The Trust Board, as proprietor, retains strategic responsibility for safeguarding and online safety across Discovery Trust. Trustees approve this policy, ensure that it reflects statutory safeguarding expectations, and seek assurance that online safety arrangements, including filtering and monitoring, are effective, proportionate, reviewed and improved where necessary. Local Advisory Boards support school-level assurance and challenge but do not replace the Trust Board's strategic safeguarding accountability.

The Trust Board is responsible for:

- Approving this Trust-wide Online Safety Policy and ensuring it is reviewed at least annually.
- Ensuring there is a named Trustee with safeguarding oversight, including online safety and filtering and monitoring assurance.
- Receiving proportionate assurance from Trust leaders about online safety risks, incidents, training, filtering and monitoring, audit activity and areas for improvement.
- Testing that schools are implementing the Trust policy through completed school addenda, assurance visits, audits and safeguarding reporting.
- Ensuring weaknesses identified through audit, review, incidents or external scrutiny are addressed through appropriate action planning.
- Maintaining sufficient knowledge to ask informed questions about online safety, filtering and monitoring, emerging technology and safeguarding risk.

Local Advisory Boards are responsible for local assurance, including:

- Reviewing the school's completed Online Safety Addendum and seeking assurance that local arrangements implement the Trust policy.
- Meeting with the headteacher, DSL and/or nominated online safety lead to understand local strengths, risks and areas for development.
- Challenging leaders about filtering and monitoring checks, curriculum delivery, training, pupil voice, local incidents and the response to identified weaknesses.
- Escalating unresolved concerns about implementation or safeguarding assurance to Trust leaders through agreed governance routes.
- Maintaining sufficient knowledge to ask informed questions about school-level online safety practice.

Trustees and relevant Local Advisory Board members must receive proportionate training or briefing on online safety, including filtering and monitoring, emerging technology and significant safeguarding risks, so that they are able to provide informed challenge and assurance. The relevant governor or advisory board member should have appropriate involvement in assurance concerning the school's annual filtering and monitoring review, without taking responsibility for technical operation or safeguarding decision-making.

4.2 Trust Online Safety Lead / Trust safeguarding leadership

The Trust Online Safety Lead, working as part of the Trust safeguarding leadership structure, provides strategic support, guidance and assurance for online safety across Discovery Trust. This role supports schools with implementation and improvement but does not remove the accountability of headteachers, DSLs or local leaders for day-to-day practice within their schools.

- Maintaining and reviewing this Trust Online Safety Policy and associated addendum template.

- Providing Trust-wide guidance, training and updates for school leaders, DSLs and relevant colleagues.
- Supporting schools with complex online safety concerns, emerging risks and safeguarding escalation where required.
- Coordinating Trust-level assurance activity, including review of school addenda, audit outcomes, filtering and monitoring evidence, training records and improvement actions.
- Reporting relevant trends, risks, strengths and weaknesses to Trust executive leaders and Trustees.
- Working with IT and safeguarding colleagues to ensure online safety, filtering and monitoring, cyber security and AI-related risks are considered together.
- Reviewing national guidance and significant developments so that Trust expectations remain current and proportionate.
- Establishing and reviewing proportionate Trust-wide online safety training and briefing expectations, including induction, annual updating, role-specific training and additional updates where significant risks, incidents, technology changes or national guidance require them.
- Considering the effectiveness and impact of online safety training through Trust assurance activity, rather than relying only on evidence that training has taken place.

Trust-level assurance may include audits, school visits, review of records, pupil and colleague voice, incident analysis and consideration of external tools or frameworks where these add value. Schools are not required to pursue external accreditation unless this is agreed by the Trust as part of a separate improvement priority.

4.3 Headteachers / Principals and senior leaders

Headteachers and Principals are accountable for ensuring this policy is implemented consistently within their school. They must ensure that online safety is led as part of safeguarding, understood by colleagues and pupils, supported by effective systems, recorded locally, reviewed regularly and reported through appropriate school and Trust assurance routes.

Headteachers / Principals and senior leaders are responsible for:

- Ensuring the school completes and annually reviews the School Online Safety Addendum.
- Ensuring there is a named senior leader responsible for filtering and monitoring standards and that this responsibility is recorded locally.
- Ensuring the DSL has appropriate involvement in online safety, filtering and monitoring, incident response and curriculum planning.
- Ensuring colleagues receive online safety training, including how to report online safeguarding concerns.
- Ensuring new colleagues, relevant volunteers and other appropriate adults receive online safety expectations as part of induction, and that colleagues receive an appropriate substantive online safety update at least annually, supported by additional updates where emerging risks, incidents, local safeguarding intelligence, technological change or revised guidance make this necessary.

-
- Ensuring role-specific training or briefing is provided for DSLs, the senior leader responsible for filtering and monitoring, relevant IT colleagues and others with significant online safety responsibilities, so that competence and understanding are matched to role.
  Ensuring pupils receive age-appropriate online safety education through the curriculum and wider safeguarding work.
- Ensuring online safety incidents are recorded, reviewed and escalated in line with safeguarding, behaviour, data protection, cyber security or conduct procedures as appropriate.
- Ensuring local arrangements for mobile phones, smart watches, personal devices and schoolowned devices are clear, communicated and consistently implemented.
- Ensuring serious concerns, including concerns involving adults, are escalated through the correct Trust and statutory routes.
- Reporting implementation, risks, incidents and improvement actions to the Local Advisory Board and Trust as required.

4.4 School Online Safety Lead / Designated Safeguarding Lead responsibilities

The school's online safety leadership must sit within, or be directly connected to, the Designated Safeguarding Lead team. The DSL retains lead responsibility for safeguarding concerns arising from online activity. Where a school appoints a separate Online Safety Lead, that colleague must work under the safeguarding oversight of the DSL and must not operate as a separate route for safeguarding decision-making.

- Lead the school's safeguarding response to online safety concerns, including concerns identified through filtering and monitoring systems.
- Ensure colleagues understand that online safety concerns must be reported through safeguarding procedures and recorded on the school's safeguarding recording system where appropriate.
- Work with the headteacher or principal and the senior leader responsible for filtering and monitoring to ensure local arrangements are effective, proportionate and reviewed.
- Understand the filtering and monitoring systems used by the school, including how alerts are generated, received, reviewed, recorded and escalated.
- Review filtering and monitoring information regularly with relevant senior and technical colleagues, identifying safeguarding themes, weaknesses, unmet needs or escalation requirements.
- Ensure online safety incidents are considered through a safeguarding lens, including where behaviour, bullying, child-on-child abuse, exploitation, harassment, sexualised behaviour, discrimination, self-harm, radicalisation, AI misuse or harmful content may be involved.
- Ensure risks for pupils with SEND, pupils with social workers, pupils experiencing mental health difficulties, pupils who are absent from education and other vulnerable pupils are considered when reviewing online safety arrangements.
- Contribute to curriculum planning so that online safety education responds to current risks, local context, pupil voice and safeguarding intelligence.
- Support colleagues with advice, training and updates on online safety, emerging risks and safeguarding reporting expectations.

-
- Ensure serious or complex online safety concerns are escalated to the headteacher or principal, Trust safeguarding leadership, statutory agencies, police, CEOP or other relevant services where appropriate.
- Ensure pupil voice is considered as part of the school's online safety development, assurance and improvement work.
  Provide proportionate reports to the headteacher or principal, Local Advisory Board and Trust safeguarding leadership on online safety risks, themes, incidents, training, assurance and improvement actions.

4.5 School IT colleagues, Trust IT colleagues and external IT providers

School IT colleagues, Trust IT colleagues and external IT providers play an important role in supporting safe, secure and effective digital systems. Their role is technical and operational; safeguarding decisions remain the responsibility of the headteacher or principal, DSL and relevant senior leaders. IT colleagues must work closely with safeguarding leaders so that technical controls, alerts, incidents and system weaknesses are understood and acted on appropriately.

- Maintain secure, reliable and appropriately restricted access to school and Trust networks, systems, devices and accounts.
- Implement, maintain and review filtering and monitoring systems in line with Trust expectations, DfE standards and agreed local arrangements.
- Ensure filtering and monitoring settings are applied appropriately to users, groups, devices, locations and platforms, taking account of age, curriculum, SEND, vulnerability and safeguarding need.
- Ensure filtering systems block illegal and harmful content as far as reasonably possible, including known child sexual abuse material, terrorist content, extremist material and other inappropriate content.
- Support schools to avoid inappropriate under-blocking or over-blocking by reviewing requests, patterns, concerns and curriculum needs with senior and safeguarding leaders.
- Ensure monitoring alerts, reports and technical concerns are routed to the correct safeguarding or senior colleagues without delay and in accordance with the school's local arrangements.
- Keep records of significant filtering or monitoring changes, technical checks, incidents, weaknesses, escalations and remedial action where required.
- Record material changes to filtering arrangements proportionately, including significant blocking, allowing, exception or configuration decisions, the reason for the decision, appropriate authorisation and any required review. Sensitive technical configuration must not be included in the published policy or school addendum.
- Support the school's annual review of filtering and monitoring effectiveness by providing technical evidence, reports, configuration information and advice.
- Apply appropriate access controls, password expectations, account management, multi-factor authentication where required, patching, software management and cyber security protections.

-
- Respond promptly to suspected cyber security incidents, compromised accounts, malware, phishing, data loss, unauthorised access or attempts to circumvent filtering through VPNs, proxies, hotspots or other methods.
- Ensure new systems, platforms, applications or AI tools are not enabled or introduced without appropriate approval, safeguarding consideration, data protection consideration and technical review.
- Check filtering and monitoring arrangements on new devices, services, applications and significant system changes before they are made routinely available to pupils or colleagues. Ensure IT colleagues or external providers who receive or handle monitoring information have appropriate safeguarding and online-safety awareness so they understand when information must be escalated to the DSL.
- Where technically possible and proportionate, support monitoring arrangements that enable activity of safeguarding concern to be traced to the relevant user or account so that concerns can be assessed appropriately.
- Work within agreed escalation routes and make clear when an issue is technical, safeguarding, data protection, behaviour, professional conduct or cyber security related.

4.6 Teaching and support colleagues

Teaching, pastoral, administrative, support and other school colleagues are responsible for modelling safe, respectful and professional use of technology and for promoting safe online behaviour with pupils. They must understand that online safety concerns may be safeguarding concerns and must never be dealt with solely as an IT or behaviour matter where there is a risk of harm.

- Read, understand and follow this policy, the Trust Safeguarding and Child Protection Policy, relevant acceptable use agreements, information security expectations, communication expectations and local device arrangements.
- Attend required safeguarding and online safety training and updates, including how online concerns enter safeguarding procedures, how filtering and monitoring concerns are reported, the significance of online child-on-child abuse, sharing nudes and semi-nudes, AI-generated sexual or abusive imagery, sextortion, grooming and exploitation, radicalisation, cyber security reporting, professional boundaries and approved communication.
- Engage with additional updates where significant national, Trust or local online safety risks emerge.
- Report online safety concerns without delay through the school's safeguarding procedures where a pupil may be at risk of harm, including concerns identified through pupil disclosure, classroom activity, online behaviour, digital communication, device use, filtering or monitoring alerts.
- Record concerns accurately on the school's safeguarding recording system where required and seek DSL advice where the correct route is unclear.
- Use Trust-approved or school-approved systems, devices, platforms and communication routes when working with pupils, parents and carers.
- Maintain professional boundaries online and never use personal accounts, personal messaging services or personal social media to communicate with pupils unless this has been explicitly authorised through an approved school process.

-
- Use school-owned or approved devices and platforms for capturing, storing or sharing pupil images, recordings or personal information, in line with consent, data protection and safeguarding expectations.
- Supervise and guide pupil use of technology in lessons and activities, including pre-planned internet use, online research, AI tools, collaboration platforms and digital resources.
- Support pupils to understand safe, respectful and responsible online behaviour, including reporting concerns, protecting privacy, evaluating information critically and responding safely to harmful content or contact.
- Implement local arrangements for mobile phones, smart watches, wearable technology, personal devices and school-owned devices consistently and proportionately.
  Remain alert to attempts to bypass filtering or monitoring, including the use of VPNs, proxies, hotspots, mobile data, shared accounts or unapproved apps, and report concerns through the appropriate route.
- Challenge or report inappropriate online behaviour by adults, including boundary concerns, misuse of images, inappropriate communication, data protection concerns or conduct that may meet low-level concern, allegation, disciplinary or safeguarding thresholds.
- Ensure online safety teaching is delivered in line with curriculum expectations and adapted appropriately for pupils' age, stage, SEND, vulnerability, communication needs and lived experience.

4.7 Pupils

Pupils are expected, at an age, stage and ability appropriate level, to use technology safely, respectfully and responsibly. Schools must support pupils to understand these expectations through curriculum teaching, acceptable use agreements, pastoral support, safeguarding conversations and clear local procedures.

- Use school systems, accounts, devices, platforms and internet access in line with the pupil acceptable use agreement and school instructions.
- Treat others with respect online and offline, including when using messages, collaboration tools, gaming, social media, images, video, audio, AI tools or shared documents.
- Follow the school's local arrangements for mobile phones, smart watches, wearable technology, personal devices and school-owned devices.
- Keep passwords and account details private and avoid using another person's account, device or identity.
- Protect personal information, images and recordings and think carefully before sharing information about themselves or others.
- Report online concerns to a trusted adult without delay, including harmful content, bullying, harassment, grooming, pressure to share images, scams, sextortion, impersonation, discrimination, extremist content, self-harm content, AI-generated harm or any online behaviour that makes them feel unsafe.

-
- Seek help if they see, receive or are asked to share nudes, semi-nudes, sexualised images or AI-generated sexual imagery. Pupils must not forward, save, screenshot, upload or show such material to others.
- Use artificial intelligence tools only where this is allowed by the school and in line with teaching, safeguarding, data protection and academic integrity expectations.
- Understand that online actions can affect others and may lead to safeguarding, behaviour, criminal, disciplinary or restorative responses depending on the concern.
- Tell a trusted adult if they accidentally access unsuitable content, receive worrying contact, believe their account has been compromised, or think they have clicked on a suspicious link.
- Contribute to pupil voice activity, surveys and discussions that help the school understand online safety strengths, risks and areas for improvement.

4.8 Parents/carers

Parents and carers play an important role in helping pupils use technology safely, respectfully and responsibly. Schools will work with parents and carers to promote online safety, explain local

expectations, share safeguarding information where appropriate, and encourage early reporting of concerns.

Schools must provide parents and carers with regular, accessible information about online safety, including local expectations, reporting routes and significant emerging risks. Communication should be proportionate to the age and needs of pupils and should include targeted information, events or support where local safeguarding intelligence, incidents or identified vulnerabilities indicate that this would be beneficial. This may include school websites, newsletters, parent/carer events, curriculum information, online safety campaigns and targeted support where risks are identified.

- Support their child to follow school acceptable use agreements and local arrangements for mobile phones, smart watches, personal devices, school-owned devices and online platforms.
- Encourage their child to speak to a trusted adult if they experience harmful content, unsafe contact, online bullying, coercion, pressure to share images, scams, sextortion, AI-generated harm or any other online concern.
- Report online safety or safeguarding concerns to the school promptly, using the local reporting routes set out in the School Online Safety Addendum.
- Support the school's expectations for respectful online communication with colleagues, pupils, parents and carers.
- Use school-approved communication systems when contacting the school and avoid using personal social media or informal messaging routes to raise safeguarding concerns.
- Follow school guidance on photographs, video recordings, livestreaming and sharing images from school events, including not publishing images of other pupils without permission.
- Support age-appropriate boundaries, privacy settings, parental controls and online supervision at home where possible.
- Work with the school where individual arrangements are required because of safeguarding, medical, SEND or other agreed needs.

4.9 Community users

Community users, hirers, visitors, volunteers, contractors and external organisations who access Trust or school systems, networks, devices, platforms or premises must follow the relevant acceptable use, safeguarding, information security and visitor expectations. Access must be authorised, proportionate to the purpose of the activity and removed when no longer required.

- Community users must not access school systems, networks or devices unless this has been approved by the school.
- Where access is provided, users must comply with the relevant acceptable use agreement and any site-specific arrangements.
- Community users must not attempt to bypass filtering, monitoring, security controls or access restrictions.
- Any safeguarding, online safety, cyber security or data protection concern involving a community user must be reported to the school without delay and escalated in line with Trust procedures.
- Schools must consider online safety and safeguarding expectations when agreeing lettings, community use, external provision or third-party access to systems or premises.

5. Filtering and monitoring

Discovery Trust requires every school to have filtering and monitoring arrangements that are effective, proportionate, regularly reviewed and clearly linked to safeguarding practice. Filtering and monitoring are not solely technical controls; they are part of the Trust's safeguarding system and must help schools identify, prevent and respond to online risk.
Filtering should restrict access to harmful and inappropriate content while avoiding unnecessary overblocking that prevents pupils from accessing legitimate teaching, learning, safeguarding, health or support resources. Monitoring should help schools identify safeguarding concerns, risky behaviour, attempted access to harmful content, cyber security concerns and possible attempts to bypass controls.

5.1 Governance and accountability

- The Trust Board seeks assurance that filtering and monitoring arrangements across the Trust are effective, reviewed and appropriately linked to safeguarding.
- The Trust Online Safety Lead and Trust safeguarding leadership coordinate Trust-level assurance and identify themes, risks, support needs and improvement actions.
- The headteacher or principal is accountable for ensuring that filtering and monitoring arrangements are implemented effectively within the school.
- Each school must identify a senior leader responsible for filtering and monitoring standards. This responsibility must be recorded in the School Online Safety Addendum.
- The DSL must be involved in filtering and monitoring arrangements, including alert review, safeguarding interpretation, escalation, recording and annual review of effectiveness.
- IT colleagues and external IT providers are responsible for technical implementation, maintenance, reporting and evidence, but they do not make safeguarding decisions without appropriate senior or DSL involvement.

5.2 Minimum expectations

- Filtering and monitoring systems must be active on school networks and on school-owned devices where technically possible and proportionate.
- Schools must understand which devices, networks, accounts, locations and user groups are covered by filtering and monitoring, and where limitations exist.
- Systems must help block access to illegal and harmful content, including child sexual abuse material, terrorist content, extremist material, pornography, violent content, hate content, self-harm and suicide-related content, and other content that presents safeguarding risk.
- Settings must be age-appropriate and should take account of curriculum needs, phase, SEND, vulnerability, safeguarding need and local context.
- Schools must have a clear route for colleagues, pupils and parents/carers to report concerns about over-blocking, under-blocking, alerts, harmful content or attempts to bypass controls.
- Schools must consider filtering and monitoring when introducing new systems, platforms, apps, devices, AI tools or online services.

- Personal devices, mobile data, hotspots, VPNs, proxies and other methods used to bypass filtering or monitoring must be addressed through local device arrangements, behaviour procedures and safeguarding procedures as appropriate.

5.3 Operational checks, review and evidence

- Each school must complete and record operational filtering and monitoring checks at a frequency appropriate to its systems and risk profile. Records should show, proportionately, the date of the check, who completed it, what was checked or tested, any issue identified, resulting action, and completion or review of any action.
- Checks must consider both safeguarding effectiveness and technical operation, including whether systems are working in practice rather than merely confirming that a product has been purchased.
- Checks and reviews should establish that appropriate controls operate across relevant schoolowned devices, Trust-owned devices, user groups, accounts, networks, school sites or locations, managed devices used away from school and relevant apps or services where technically applicable. Schools must understand material limitations in coverage and how those limitations are mitigated.
- Filtering and monitoring must be considered and, where relevant, tested before new devices, services, platforms, apps or significant digital systems are rolled out.
- The DSL, senior leader responsible for filtering and monitoring, and relevant IT colleague or provider must review filtering and monitoring information regularly. Monitoring arrangements must distinguish between routine monitoring information and high-risk safeguarding alerts.
- Monitoring arrangements must enable high-risk safeguarding concerns to be brought to the attention of the appropriate safeguarding colleague without unnecessary delay. Routine monitoring information must be reviewed at a frequency appropriate to the system and risk profile, with patterns or concerns escalated where required.
- Each school must complete and record a formal review of filtering and monitoring effectiveness at least annually and whenever there is a significant change to systems, provision, technology use, safeguarding risk or statutory guidance. The review should involve, as appropriate, the headteacher or principal or responsible senior leader, the DSL, the senior leader responsible for filtering and monitoring, relevant IT colleagues or provider, and appropriate governance oversight.
- The annual review should consider effectiveness of filtering, effectiveness of monitoring, safeguarding incidents and trends, user and device coverage, under-blocking, over-blocking, circumvention attempts, system limitations, SEND and vulnerability, local risk, emerging technology including generative AI, actions from previous reviews, and whether identified actions have improved practice.
- Significant decisions to block, allow or alter access to content, services or categories must be recorded proportionately, including the safeguarding or educational rationale and appropriate approval.
- Local arrangements must identify who receives high-risk alerts, who reviews routine monitoring reports, how frequently routine information is reviewed, who covers the role during absence, how concerns reach the DSL, and how significant actions are recorded. Where

the Trust's filtering and monitoring procedure specifies a minimum reporting frequency, schools must comply with that procedure.
- Trust-level assurance may include review of school addenda, sample checks, safeguarding visit activity, audit activity, incident analysis, colleague voice, pupil voice and reports from IT or filtering and monitoring providers.

5.4 Data protection and monitoring

Filtering and monitoring arrangements must operate in accordance with applicable data protection and information governance requirements. Where technical monitoring involves the processing of personal data, schools and the Trust must ensure that appropriate privacy information is provided and that a Data Protection Impact Assessment is completed where required. Monitoring must be proportionate to the safeguarding purpose and access to monitoring information must be appropriately controlled.
Schools must consider data protection, safeguarding and information security when procuring or materially changing filtering and monitoring services.

5.5 Responding to alerts and concerns

- Filtering and monitoring alerts must be reviewed by the correct colleague or team without unnecessary delay.
- High-risk alerts indicating possible immediate or serious harm must be escalated through the school's safeguarding arrangements without unnecessary delay and must not wait for routine monitoring review.
- Schools must have contingency arrangements so that safeguarding alerts continue to be reviewed during absence of the usual alert recipient.
- Concerns that indicate possible harm, vulnerability, child-on-child abuse, exploitation, harmful sexual behaviour, suicidal ideation, self-harm, radicalisation, grooming, sextortion, AIgenerated abuse, illegal content or other safeguarding risk must be referred to the DSL and recorded through safeguarding procedures.
- Concerns that appear primarily technical, such as system failure, attempted bypassing, malware, suspicious links or compromised accounts, must be referred to IT and escalated to safeguarding or senior leaders where pupil or colleague risk may be present.
- Concerns that indicate possible data breach, cyber security incident, colleague misconduct, low-level concern or allegation must be escalated through the relevant Trust procedure.
- Schools must not rely on automated tools alone. Professional judgement, DSL oversight and proportionate investigation are required where alerts or reports indicate possible safeguarding risk.

5.6 Local information

Each school must record in its School Online Safety Addendum the filtering provider, monitoring provider, named senior leader, DSL involvement, operational check arrangements, review frequency, alert recipients, escalation route, recording arrangements and any known limitations or local variations. Schools should not include detailed technical configuration in the published addendum where this would create security risk.

6. Online safety in the curriculum

Online safety education is a core part of safeguarding, curriculum and personal development. Discovery Trust schools must provide planned, age-appropriate and developmentally appropriate online safety education through Relationships Education, Relationships and Sex Education where applicable, Health Education, computing, digital literacy, wider safeguarding work, assemblies, tutor time, pastoral support and responsive teaching following incidents or emerging risks.

Curriculum provision must help pupils understand online risk, build confidence to seek help, develop respectful online behaviour, evaluate digital information critically, protect privacy and personal information, understand consent and boundaries, and respond safely to harmful content, unsafe contact or online coercion.

Schools must ensure that online safety teaching is regularly reviewed in response to national guidance, Trust priorities, local safeguarding intelligence, pupil voice, incident patterns, technology changes and the needs of pupils within the school.

6.1 Curriculum expectations

- safe, respectful and responsible use of technology, including school systems, personal devices, online platforms and artificial intelligence tools;
- the four categories of online risk: content, contact, conduct and commerce;
- healthy online relationships, consent, privacy, boundaries, digital footprints and respectful communication;
- how to recognise and report harmful content, unsafe contact, cyberbullying, online harassment, grooming, coercion, exploitation and harmful sexual behaviour;
- risks linked to sharing nudes and semi-nudes, sexualised images, AI-generated sexual imagery, sextortion and image-based abuse;
- misinformation, disinformation, conspiracy theories, manipulated media, deepfakes and critical evaluation of online information;
- cyber security awareness, including passwords, phishing, suspicious links, compromised accounts, scams, fraud and safe handling of personal information;
- digital wellbeing, including screen use, sleep, online pressure, gaming, social media, comparison, harmful online influence and help-seeking;
- how to seek help from trusted adults, school reporting routes, CEOP, police or other appropriate services where relevant.

6.2 Age, stage and vulnerability

- Teaching must be matched to pupils' age, stage of development, communication needs, lived experience and level of independence online.
- Schools must adapt teaching for pupils with SEND, pupils with social workers, pupils experiencing mental health difficulties, pupils who are absent from education, pupils at risk of exploitation and other vulnerable pupils.

- Schools must consider whether targeted teaching, pastoral support or individual safety planning is required where pupils are at increased risk online.
- Teaching should avoid victim-blaming and should make clear that pupils can seek help even if they are worried, embarrassed, have broken a rule or have been pressured into something online.

6.3 Artificial intelligence, synthetic media and emerging technology

- Pupils should be taught, where age and stage appropriate, that AI-generated content may be inaccurate, biased, misleading, manipulated or harmful.

- Pupils should understand that AI can be used to create or alter text, images, audio, video, online profiles and messages, including deepfakes and impersonation.
- Pupils must be taught that creating, requesting, possessing, sharing or threatening to share nude, semi-nude, sexualised, abusive or humiliating AI-generated imagery can cause serious harm and may be criminal.
- Pupils should understand that personal, sensitive, safeguarding or confidential information must not be entered into unapproved AI systems.
- Schools must teach pupils how to use approved AI tools responsibly, where AI use is permitted, including expectations for academic integrity and checking accuracy.

6.4 Local curriculum recording and assurance

- Each school must record in its Online Safety Addendum how online safety is delivered locally and who is responsible for curriculum oversight.
- Curriculum leaders, DSLs and senior leaders should review online safety provision together so that teaching reflects safeguarding intelligence, pupil voice and local risk.
- Schools should retain proportionate evidence of curriculum delivery, such as curriculum maps, lesson materials, assemblies, campaigns, pupil voice, parent/carer engagement and records of responsive teaching.
- Trust assurance may include review of curriculum documentation, safeguarding visit activity, pupil voice, colleague voice, incident analysis and review of local addenda.

7. Artificial intelligence and emerging technology

Discovery Trust recognises that artificial intelligence, generative AI, synthetic media and emerging technologies can support learning, creativity, accessibility and productivity when used appropriately. These tools can also create safeguarding, data protection, professional conduct, curriculum, behaviour, equality, cyber security and reputational risks. The Trust's approach is therefore cautious, proportionate and safeguarding-led.

AI tools must not be introduced, promoted or used with pupils unless they are approved through the appropriate Trust or school process and have been considered for safeguarding, data protection, age suitability, accessibility, educational purpose and technical risk.

7.1 Core expectations

- Colleagues and pupils must use AI tools only where this is permitted by the Trust or school and in line with approved guidance.
- Personal, sensitive, confidential, safeguarding, medical, SEND, HR, disciplinary, allegation, pupil record or identifiable family information must not be entered into unapproved AI systems.
- Colleagues must not use AI-generated content as a substitute for professional judgement, safeguarding decision-making, DSL oversight, legal advice, clinical advice or statutory processes.
- AI-generated information must be checked for accuracy, bias, context, source reliability and suitability before being used in teaching, communication, reports or decision-making.

- AI tools must not be used to create, alter, imitate or distribute images, audio, video, messages or profiles in ways that could mislead, humiliate, harass, exploit, impersonate or harm another person.
- Schools must consider age restrictions, terms of service, consent, accessibility, equality, curriculum purpose and data protection before pupils are allowed to use any AI platform.

7.2 Safeguarding risks

- deepfakes, synthetic media, impersonation and manipulated images, audio or video;
- AI-generated nude, semi-nude, sexualised, abusive or humiliating imagery;
- online coercion, grooming, manipulation, sextortion or blackmail supported by AI tools;
- misinformation, disinformation, conspiracy content, hoaxes and hallucinated content presented as fact;
- bias, discrimination, stereotyping or unfair treatment in AI-generated content or outputs;
- cyberbullying, harassment, misogyny, hate, discrimination or threatening communication supported by AI tools;
- plagiarism, academic dishonesty or inappropriate reliance on AI-generated work;
- copyright, intellectual property, ownership and attribution concerns;
- privacy, data protection and confidentiality risks arising from inputting information into AI systems;
- malicious use of AI to support scams, phishing, social engineering, fraud or cyber security attacks.

7.3 Colleague use of AI

- Colleagues must follow Trust and school guidance before using AI tools for planning, teaching, assessment, communication, reports, administration or resource creation.
- Colleagues must not enter identifiable pupil, parent/carer, colleague, safeguarding, medical, SEND, conduct, complaint or confidential Trust information into unapproved AI tools.
- AI may support drafting, summarising, planning or accessibility where approved, but colleagues remain responsible for accuracy, appropriateness, professional tone, confidentiality and final decisions.
- Colleagues must be alert to inaccurate, biased, invented or inappropriate AI outputs and must not present AI-generated content as verified professional information without checking it.
- Any colleague use of AI that creates a safeguarding, conduct, confidentiality, copyright, equality, data protection or reputational concern must be reported through the appropriate route.

7.4 Pupil use of AI

- Pupils may use AI tools only where this is permitted by the school and supervised or guided in line with age, stage, curriculum purpose and safeguarding expectations.
- Pupils must be taught that AI-generated content can be inaccurate, biased, misleading, manipulated or harmful.

-
- Pupils must not use AI to impersonate others, create abusive content, generate or alter sexualised images, bully, harass, deceive, plagiarise, access harmful content or bypass school systems.
  Pupils must not enter personal, sensitive or confidential information about themselves or others into unapproved AI platforms.
- Schools must respond to AI misuse through safeguarding, behaviour, anti-bullying, data protection, cyber security or criminal procedures as appropriate.

7.5 Approval, review and local recording

- Schools must record locally approved AI tools or services in the School Online Safety Addendum or another agreed local record.
- Before approving a new AI tool, leaders must consider safeguarding, educational purpose, data protection, information security, accessibility, equality, age suitability, terms of service, retention of data and whether filtering or monitoring controls are needed.
- Trust safeguarding, IT and data protection colleagues should work together where AI use raises significant risk or requires Trust-level approval.
- AI-related concerns must be reported and recorded through the relevant safeguarding, behaviour, data protection, cyber security or conduct process.
- AI guidance must be reviewed as technology, national guidance and Trust practice develop.

8. Harmful online activity and safeguarding escalation

Discovery Trust recognises that online harm can involve behaviour between pupils, adults, unknown individuals, organised groups, commercial actors or technology-enabled systems. Online harm may occur inside or outside school, on school systems or personal devices, and may be connected to offline abuse, exploitation, bullying, harassment, discrimination or vulnerability.
All online safety concerns must be considered through a safeguarding lens. Colleagues must not treat online incidents solely as IT or behaviour matters where there is any indication of risk, harm, vulnerability, coercion, exploitation, discrimination, sexualised behaviour, radicalisation, criminal activity, adult conduct concern, data breach or cyber security risk.

8.1 Types of harmful online activity

- cyberbullying, online harassment, abuse, intimidation, humiliation, misogyny, hate, discrimination or threatening communication;
- child-on-child abuse, harmful sexual behaviour, sexual harassment, sexual violence, pressure to share images, sharing nudes and semi-nudes, image-based abuse and AI-generated sexual or abusive imagery;
- grooming, exploitation, coercion, sextortion, online blackmail, stalking, doxxing, impersonation and privacy breaches;
- exposure to or promotion of pornography, violent content, self-harm content, suicide-related content, eating-disorder content, extremist material, terrorist content, harmful online communities or radicalising influence;

-
- scams, fraud, gambling, inappropriate commercial activity, phishing, social engineering, malicious communications, account compromise, malware, hacking or cybercrime;
- misinformation, disinformation, conspiracy content, deepfakes, synthetic media, manipulated content or harmful online influence;
- inappropriate use of social media, messaging, livestreaming, gaming, video conferencing, online learning platforms, AI tools or school communication systems;
  attempts to bypass filtering, monitoring or security controls using VPNs, proxies, hotspots, mobile data, shared accounts or unapproved applications.

8.2 Safeguarding escalation

- Where an online concern indicates that a pupil is at risk of harm, the concern must be reported to the DSL without delay and recorded on the school's safeguarding recording system.
- Where an online concern involves child-on-child abuse, harmful sexual behaviour, sexual harassment, sexual violence, sharing of nudes or semi-nudes, AI-generated sexual imagery, coercion or exploitation, the DSL must lead the response in line with the Safeguarding and Child Protection Policy and relevant national guidance.
- Where an online concern may involve an adult working with pupils, including professional boundary concerns, inappropriate communication, misuse of images, low-level concerns or allegations, the matter must be escalated through the Trust's managing allegations, low-level concerns or conduct procedures.
- Where an online concern may involve criminal activity, illegal content, radicalisation, terrorism, child sexual exploitation, child criminal exploitation, cybercrime, sextortion or malicious communications, the DSL or headteacher must consider whether police, CEOP, local authority children's social care, Channel, Cyber Choices or other specialist advice is required.
- Where an online concern may involve personal data, confidentiality, unauthorised access, compromised accounts, cyber security or system failure, leaders must follow the relevant data protection and cyber security reporting routes as well as safeguarding procedures where risk to pupils or colleagues is present.

8.3 Recording, evidence and pupil support

- Records must show the nature of the concern, who was involved, what immediate action was taken, what safeguarding assessment was made, who was informed, what referrals or advice were sought, what support was offered and what follow-up or review is required.
- Colleagues must not view, copy, print, forward, save or share nude, semi-nude, sexualised, abusive or illegal imagery of pupils. Where such material is suspected, the device or account should be secured where safe to do so and the concern reported immediately to the DSL.
- Evidence should be preserved safely and proportionately. Leaders should seek advice from the DSL, police or other relevant agency before deleting, altering or sharing material that may be evidence of harm or criminal behaviour.

-
- Pupils affected by online harm must be listened to, reassured, supported and protected from further harm. Responses must avoid victim-blaming and must consider the pupil's age, SEND, communication needs, vulnerability, mental health, family context and wider safety.
- Schools should consider whether wider action is required following an incident, including curriculum response, parent/carer communication, pupil voice, technical review, filtering and monitoring review, behaviour response, risk assessment or referral to external agencies.

9. Devices and acceptable use

Discovery Trust expects all technology to be used safely, lawfully, respectfully and for appropriate educational, professional or operational purposes. Device use must support safeguarding, learning,

communication and operational effectiveness while reducing risks linked to inappropriate access, recording, sharing, communication, distraction, data loss and harm.

9.1 Acceptable use

- All users must follow the relevant acceptable use agreement before accessing Trust or school networks, systems, devices, accounts, platforms or internet services.
- Acceptable use expectations must be age-appropriate, clearly communicated and reviewed when systems, risks or local arrangements change.
- Discovery Trust maintains separate Acceptable Use Agreements appropriate to the age, stage, ability and role of users. These agreements support implementation of this policy and may include versions for different pupil phases, colleagues and other users as appropriate. Schools must use the current Trust-approved version or an approved accessible adaptation and must not weaken the safeguarding expectations contained within it.
- Pupil Acceptable Use Agreements must be communicated in a way pupils can understand, taking account of age, development, SEND and communication need. Where acknowledgement or agreement is required, schools may use an appropriate local mechanism.
- Users must not access, create, store, transmit or share illegal, harmful, discriminatory, abusive, sexualised, extremist, violent, fraudulent or otherwise inappropriate material.
- Users must not attempt to bypass filtering, monitoring, security controls or access restrictions, including through VPNs, proxies, hotspots, mobile data, shared accounts or unapproved applications.
- Breaches of acceptable use may be addressed through safeguarding, behaviour, conduct, disciplinary, data protection, cyber security or criminal procedures as appropriate.

9.2 Trust-owned and school-owned devices

- Trust-owned and school-owned devices must be managed in line with safeguarding, information security, filtering, monitoring, asset management and data protection expectations.
- Devices must be allocated, used, stored, returned and maintained in accordance with local procedures.
- Where pupils take school-owned devices home, schools must set clear arrangements for use, supervision, filtering, monitoring, reporting concerns, damage, loss and return.
- Colleagues must use approved devices and platforms for school business wherever possible and must protect confidential and personal information at all times.
- Lost, stolen, compromised or damaged devices must be reported promptly through the school's local route and, where necessary, through cyber security or data protection procedures.

9.3 Personal devices, mobile phones and smart technology

- Schools covered by the Department for Education's statutory mobile phones in schools guidance must have regard to the expectation, applicable from 1 September 2026, that pupils should not have access to or use mobile phones throughout the school day, including lessons, movement between lessons, breaktimes and lunchtimes. Any lawful, necessary and proportionate adaptations or exceptions must be agreed and recorded through local arrangements.
  Local arrangements must take account of age range, phase, SEND, disability, medical need, safeguarding need, transport arrangements, post-16 provision, specialist provision and individual circumstances. Exceptions must not be based simply on pupil preference.
- Smart watches and other personal interactive communication devices may be addressed through the same local arrangements where their functionality creates similar safeguarding, behaviour or distraction risks.
- Pupils must not use personal devices to take, store or share images, video, audio or personal information in school unless this is explicitly permitted by the school for a legitimate purpose.
- Colleagues must not use personal devices to contact pupils or parents/carers, capture pupil images or recordings, store pupil information or conduct school business unless there is an exceptional, authorised and recorded reason.
- Personal devices must not be used to bypass filtering, monitoring or school communication systems.
- Schools must record local device arrangements, including exceptions, in the School Online Safety Addendum or a referenced local procedure.

9.4 Cameras, images, recordings and livestreaming

- Images, video and audio recordings of pupils must be captured, stored and shared only for approved educational, safeguarding or operational purposes and in line with consent, data protection and safeguarding expectations.
- School-owned or approved devices and platforms should be used for pupil images and recordings wherever possible.
- Colleagues must not store pupil images, recordings or personal information on personal devices, personal cloud accounts or unapproved platforms.
- Parents/carers and visitors must follow school guidance on photography, filming, livestreaming and sharing images at school events.
- Any concern about inappropriate image use, recording, livestreaming, sharing, deepfakes, AIgenerated imagery or image-based abuse must be reported as a safeguarding concern where harm or risk may be present.

9.5 Searching, confiscation and examination of devices

- Where authorised colleagues have reasonable grounds to believe that a digital device contains evidence of misconduct, bullying, safeguarding concern or criminal activity, the

school may search, confiscate and examine devices in accordance with statutory guidance, the Ready to Learn Policy, searching and confiscation procedures, and safeguarding procedures.

- Before searching a device, colleagues should consider urgency, risk, proportionality and whether advice from the headteacher, DSL or another appropriate senior leader is required.
- Where colleagues suspect that a device may contain a nude or semi-nude image of a pupil, including an image generated or manipulated using artificial intelligence, they must not view, copy, print, forward, share or save the image. The device should be secured where safe to do so and the concern reported immediately to the DSL.
- Where content may be evidence of a criminal offence, leaders must preserve evidence appropriately and seek advice from the DSL, police or other relevant agency before deleting, altering or sharing material.

10. Communication and social media

Discovery Trust expects all online and digital communication connected to school or Trust activity to be professional, respectful, safeguarding-led and conducted through approved systems wherever possible. Communication arrangements must protect pupils, maintain professional boundaries, support effective engagement with parents and carers, and reduce risks linked to informal contact, personal accounts, social media, messaging apps and image sharing.

10.1 Professional boundaries and approved communication

- Colleagues must use Trust-approved or school-approved communication systems when communicating with pupils, parents, carers, colleagues, governors or external partners about school business.
- Colleagues must not use personal social media accounts, personal email, personal messaging services or personal mobile numbers to communicate with pupils unless there is an exceptional, authorised and recorded reason.
- Communication with pupils must be purposeful, proportionate, transparent and linked to education, safeguarding, pastoral support or school activity.
- Colleagues must maintain professional boundaries at all times and must report any communication concern that may indicate grooming, exploitation, harassment, inappropriate contact, low-level concern, allegation or breach of conduct expectations.
- Schools must record locally approved pupil, parent/carer and colleague communication platforms in the School Online Safety Addendum.

10.2 Social media

- Official school or Trust social media accounts must be authorised, managed and monitored in accordance with Trust communication, safeguarding, data protection and conduct expectations.

- Personal social media accounts must not be used to communicate with pupils or to discuss confidential, safeguarding, pupil, family, colleague or Trust information.
- Colleagues must not accept or initiate social media contact with pupils through personal accounts.
- Colleagues should be aware that personal online activity may affect professional reputation, safeguarding trust and public confidence where it is linked to their role or the Trust.
- Any concern about online conduct by a colleague must be reported through the appropriate conduct, low-level concern, allegation or safeguarding procedure.
- Pupils must be supported to understand respectful and safe use of social media, including privacy, image sharing, harmful content, online influence, misinformation, bullying, harassment and reporting concerns.

10.3 Messaging, video conferencing, livestreaming and online learning

- Messaging, video conferencing, livestreaming and online learning must take place through approved platforms and in line with safeguarding, behaviour, data protection and professional conduct expectations.
- Schools must set clear expectations for supervision, recording, attendance, use of cameras and microphones, chat functions, screen sharing, pupil conduct and reporting concerns.
  Colleagues must not record lessons, meetings or pupil interactions unless this is authorised and managed in line with safeguarding, data protection and retention expectations.
- Parents and carers should be informed of relevant expectations when pupils take part in remote learning, livestreamed activity or online communication from home.
- Any concern arising from online learning, video conferencing or livestreaming must be reported through the appropriate safeguarding, behaviour, data protection, cyber security or conduct route.

10.4 Communication with parents and carers

- Schools must identify approved systems for communicating with parents and carers and record these in the School Online Safety Addendum.
- Safeguarding concerns should be raised through the school's safeguarding routes rather than through informal social media or personal messaging.
- Communication with parents and carers must be professional, respectful, accessible and proportionate.
- Schools should provide guidance to parents and carers about reporting online safety concerns, including concerns involving harmful content, contact, bullying, image sharing, AI-generated harm, sextortion, scams or unsafe communication.
- Schools should use significant online safety incidents and emerging local trends to consider whether wider parent/carer communication or education is required.

11. Remote learning

Remote learning, blended learning and online learning must be delivered through approved platforms and in line with this policy, the Trust Safeguarding and Child Protection Policy, data protection expectations, behaviour expectations, communication expectations and any relevant local remote learning procedures.

Schools must consider safeguarding, privacy, accessibility, equality, data protection, filtering, monitoring and cyber security before introducing or changing remote learning platforms, online learning tools, video conferencing systems or digital resources. Pupils must not be required to use unapproved platforms or personal accounts for school-directed learning.

Where school-owned devices are used for remote learning, schools must ensure that appropriate security, filtering, monitoring and safeguarding arrangements are in place as far as technically possible. Where pupils use devices or internet connections not owned or managed by the school or Trust, schools must provide safeguarding advice to parents and carers but cannot directly manage technical controls on those devices or networks.

Remote learning arrangements must include clear expectations for:

- which platforms and accounts pupils and colleagues should use;
- attendance, supervision, contact, engagement and welfare checks;
- camera, microphone, chat, screen-sharing and recording expectations;
- professional boundaries between colleagues and pupils;
- how pupils, colleagues and parents/carers report safeguarding or online safety concerns;
- how concerns arising during remote learning are recorded and escalated;
- how parents and carers are informed about what pupils are being asked to access and who they may interact with online;
- reasonable adjustments and additional support for pupils with SEND, pupils with social workers, pupils experiencing vulnerability and pupils who may be digitally excluded.

Schools should encourage parents and carers to use age-appropriate parental controls, privacy settings, safe-search settings and supervision at home where possible. Parents and carers should also be directed to trusted online safety resources and reminded to contact the school promptly if they have concerns about harmful content, unsafe contact, cyberbullying, image sharing, AI-generated harm, scams, sextortion or online behaviour linked to remote learning.

12. Policy review and assurance

The Trust Online Safety Policy will be reviewed centrally at least annually and whenever there is a significant change in statutory guidance, national expectations, safeguarding risk, technology, Trust systems, cyber security arrangements or operational practice. The Trust Board approves the substantive policy. Schools must not rewrite the Trust policy locally.

Each school must complete and review its School Online Safety Addendum at least annually and whenever significant local arrangements change. This includes changes to DSL responsibilities, filtering and monitoring systems, IT providers, local device arrangements, communication platforms, approved AI tools, curriculum delivery, reporting routes or relevant local safeguarding risks.

12.1 Trust assurance

- review of completed School Online Safety Addenda;
- review of filtering and monitoring arrangements, annual effectiveness reviews, operational checks and evidence of action taken;
- analysis of online safety incidents, safeguarding themes, harmful online activity, child-on-child abuse, AI-related concerns, cyber security concerns and data protection links;
- review of colleague training, DSL oversight, curriculum delivery, pupil voice and parent/carer engagement;
- Assurance activity should consider whether relevant colleagues understand their online safety responsibilities and reporting routes, rather than relying solely on evidence that training has been attended. This may be evidenced proportionately through safeguarding discussions, audit or visit activity, colleague voice, scenario-based checks, supervision, review following incidents or other suitable quality assurance.
- Assurance should also consider whether parents and carers know how to report online concerns, whether communication reflects current and local online risks, and whether targeted engagement has been provided where required. This may be sampled proportionately.
- safeguarding visits, audits, quality assurance activity and reports from schools or external providers;
- reporting to Trust executive leaders and Trustees on strengths, risks, themes, compliance, assurance findings and improvement actions.

12.2 School assurance

- ensure the addendum is accurate, complete and reviewed by appropriate senior, safeguarding and technical leaders;
  retain proportionate evidence that local arrangements are implemented, including filtering and monitoring review records, training records, curriculum evidence, incident records and local action plans;
- report online safety risks, incidents, themes and improvements to the Local Advisory Board and Trust as required;
- act promptly where review, audit, incident analysis, pupil voice, colleague voice or external scrutiny identifies a weakness;
- ensure actions are allocated to named colleagues, given realistic timescales and reviewed for completion and impact.

12.3 Improvement and escalation

Where assurance activity identifies a concern, weakness or gap, the school must agree proportionate action and escalate the matter where necessary. Serious safeguarding, cyber security, data protection, conduct or compliance concerns must be escalated immediately through the relevant Trust and statutory routes. The purpose of review and assurance is not simply to confirm that a policy exists, but to test whether responsibilities, systems, escalation and local implementation are working in practice.

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	Greystoke Primary School
Headteacher / Principal	Ronnie Richardson
DSL and Deputy DSLs	DSL: Ronnie Richardson Deputy DSL: Lizzie Whitmore, Kerry Bishop, Diane Resende
Nominated safeguarding link governor/advisory board member	Sam Belson
Local IT lead/contact	Trust IT service desk Mike Sanderson (CTO)
External IT provider, if applicable	Trust-approved external IT support provider, where required.

13. Filtering and monitoring

Filtering system/provider	Sophos filtering system, 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	Lizzie Whitmore (Deputy Head & DSL) supported by other DSLs and Trust IT.
DSL involvement in filtering and monitoring	Reviewing 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, Deputy and Trust IT Service Desk.
Who reviews alerts and how frequently	High-risk alerts are reviewed on the same working day. Routine monitoring reports are reviewed weekly by the Deputy and any actions are recorded**.**
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.
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 review.
Date of most recent formal filtering and monitoring effectiveness review	
Participants in the review and governance oversight	Headteacher, DSL report number of captures and any significant issues to the advisory board.
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 Deputy and Headteacher. Routine reports are reviewed weekly.
Location of significant filtering, blocking, allowing or exception decision records	Recorded in the filtering and monitoring review log with SENSO, 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. School signpost: Trust Data Protection folder.**

14. Devices and mobile technology

Local mobile phone arrangements	Pupils do not use mobile phones during the school day. Phones (only Y5/6) 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.
Pupil-owned devices / BYOD	BYOD is not permitted for pupils.
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	N/A
Agreed exceptions for safeguarding, medical, SEND or other needs	N/A

15. 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/carer communication systems	Arbor, school email, school website, MS Teams 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 account managed by authorised office member of staff. 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, Blended Learning/Computing Lead and DSLs.
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/carer online safety communication and local reporting route	Online safety messages are shared through newsletters, parent emails and the school website. Concerns should be reported to the DSL via the

	school office or safeguarding email. Online safety parent workshop delivered last academic year.
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 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.

16. Reporting and local escalation

How pupils report online safety concerns	Pupils report to any trusted adult or in 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 through 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.

17. Local circumstances and review

Age range / phase considerations	**All of the above is relevant to the primary setting.**
SEND, specialist or alternative provision considerations	**As above**
Residential, post-16 or other specialist arrangements, if applicable	**N/A**
Identified local safeguarding risks relevant to online safety	-Online recruitment to county lines -Grooming through social media - Sharing of inappropriate images
Date addendum completed	**September 2026**
Date addendum reviewed	**September 2027**
Reviewed by	