



Head Teacher: Kirsten MacLeod

Newham PRUs

Online Safety Policy

Reviewed by Teacher in charge of Digital Strategy
Reviewed policy agreed by Headteacher on: Autumn 2026
Reviewed policy shared with staff: Autumn 2026
Policy to be reviewed again on: Autumn 2027

Contents

What's different about this policy for 2026/27?

Introduction

- Key people / dates
- What is this policy?
- Who is it for; when is it reviewed?
- Who is in charge of online safety?
- What are the main online safety risks today?
- How will this policy be communicated?

Overview

- Aims
- Further Help and Support
- Scope

Roles and responsibilities

Education and curriculum

Handling online-safety concerns and incidents

- Sharing Nudes and Semi-Nudes
- Generative AI, Deepfakes, and Sextortion
- Priority Areas (Upskirting, Bullying, Sexual Violence & Harassment)
- Misuse of school technology

Cyber security and Data Protection

Appropriate filtering and monitoring

Electronic communications and Cloud platforms

Digital images, video, and Social Media

Device usage and Mobile Phones

Searching and confiscation

Appendices

What's different about this policy for 2026/27?

This policy has been updated for the **Autumn 2026 to Autumn 2027** academic year to reflect the latest statutory guidance from **Keeping Children Safe in Education (KCSIE) 2026** and current UK legislation. Online safety is an integral part of safeguarding and requires a whole-school, cross-curricular approach.

Key Statutory Updates for 2026/2027

- **Mandatory Annual Review of Filtering and Monitoring:** SLT, supported by the DSL and Network Manager, must execute and formally record a whole-school review of technical filtering and active monitoring systems at least once per academic year.
- **5Cs Risk Framework & Generative AI:** The policy fully adopts the updated risk framework incorporating **Context** alongside Content, Contact, Conduct, and Commerce. Generative AI risks—including AI chatbots, deepfakes, nudification apps, and synthetic CSAM—are explicitly integrated into filtering, monitoring, and conduct protocols.
- **Default Mobile-Free Environment:** Aligned with statutory directions, Newham PRUs enforces a strict, mobile-phone-free environment by default during school hours.
- **KCSIE Training Mandate:** All staff—including support, administrative, and agency staff—must read **Part One of KCSIE 2026** in full.

Introduction

Key people / dates

Role	Lead Name / Contact
Designated Safeguarding Lead (DSL)	Yasmine Dhillon
Safeguarding Team (DDSLs)	Liburd Henry, Laura O'Donnell, Phoebe Esdaile, Athena Tsioullou, Kacey Cuskelly, Beverley Drake, Ali Said, Tim Butler
Designated Safeguarding Manager	Laura O'Donnell (DDSL)
Online-Safety Lead	Luis Cravioto
Online-Safety / Safeguarding Link Governor	Kathryn Randall-Curtis
PSHE / RSHE Lead	Ricky Sparham (DHT)
Network Manager / Technical Support	Terry Carter / RM
Associate Data Protection Officer (ADPO)	Mira Gohil
Date Policy Reviewed / By	Autumn 2026 – Kirsten MacLeod
Date of Next Review	Autumn 2027

What is this policy?

Online safety is a fundamental dimension of safeguarding and requires a whole-school, cross-curricular approach. Written in compliance with **KCSIE 2026**, *Teaching Online Safety in Schools*, statutory RSHE guidance, and the Data Protection Act 2018, this policy operates alongside our Child Protection & Safeguarding Policy. Any online safety concern must be escalated via our central safeguarding software (CPOMS/Safeguard).

Who is it for; when is it reviewed?

This policy applies to all staff, management committee members, pupils, parents/carers, supply tutors, contractors, and visitors. It undergoes a full formal annual review in Autumn, with immediate interim amendments as digital risks or statutory guidance evolve.

Who is in charge of online safety?

The Headteacher holds overall accountability, while the Designated Safeguarding Lead (Yasmine Dhillon) holds operational responsibility for digital safeguarding, including understanding and auditing technical filtering and monitoring systems (WebScreen 3, RM SafetyNet, and LGfL's SENSO). Luis Cravioto serves as the dedicated Online-Safety Lead.

What are the main online safety risks today?

Risks are evaluated using the expanded **5Cs Framework**:

- **Content:** Exposure to illegal or harmful material including extreme violence, misogyny, radicalization, fake news, and synthetic/AI-generated sexual imagery.
- **Contact:** Harmful interactions with unknown adults, peers, or automated systems—including adult grooming, criminal exploitation (CCE/County Lines), and unregulated AI companion chatbots.
- **Conduct:** Personal behaviors causing harm, such as cyberbullying, non-consensual image sharing, creating deepfakes, and digital harassment.
- **Commerce:** Exposure to financial exploitation, online gambling, micro-transactions, phishing, and financial sexual extortion (*sextortion*).
- **Context:** Navigating misinformation, verifying digital authenticity, and critically evaluating AI-driven content.

How will this policy be communicated?

This policy is published on the school website, stored on the staff drive, embedded in September INSET briefs, integrated into staff/pupil induction, and translated into tailored Acceptable Use Policies (AUPs) signed annually by staff, students, and parents.

Overview

Aims

- Establish clear expectations for safe and responsible digital behavior across all platforms and devices.
- Protect vulnerable learners (SEND, CCE/CSE risk cohorts, and remote/outreach pupils) through tailored technical and pastoral controls.
- Empower staff to identify, manage, and escalate online safety incidents immediately.
- Align institutional technology usage with statutory GDPR, cyber security, and safeguarding mandates.

Further Help and Support

All internal incidents must be logged on Safeguard/CPOMS and reported to the DSL team.

External support routes include:

- **LGfL Incident Escalation:** reporting.lgfl.net
- **Professionals' Online Safety Helpline (POSH):** 0344 381 4772 / helpline@saferinternet.org.uk
- **NSPCC Whistleblowing Helpline:** 0800 028 0285

Scope

This policy applies to all digital interactions on school grounds, school devices, remote/outreach learning networks (DRMO/Blueband), personal devices connected to school Wi-Fi, and off-site online behavior that impacts the safety or reputation of the Newham PRUs community.

Roles and responsibilities

- **Headteacher (Kirsten MacLeod):** Maintains overall institutional responsibility for digital safeguarding, ensures adequate funding/resources for filtering/monitoring, oversees allegations against staff (liaising with LADO), and guarantees statutory website compliance.
- **Designated Safeguarding Lead (Yasmine Dhillon):** Retains lead operational responsibility for digital safety; oversees filtering/monitoring alert logs; leads triage on Safeguard/CPOMS; coordinates external referrals (MASH, Police, CEOP); and ensures cross-curricular online safety delivery.
- **Online-Safety Lead (Luis Cravioto):** Leads day-to-day online safety operational coordination,

pupil digital safety initiatives, and staff support.

- **Governing Body / Link Governor (Kathryn Randall-Curtis):** Reviews policy efficacy annually; ensures SLT conducts dynamic filtering audits; verifies board safeguarding training; and holds SLT accountable for statutory compliance.
- **All Staff:** Maintain continuous vigilance; read Part 1 of KCSIE 2026; enforce AUPs and mobile restrictions; thread online safety through teaching; and report any concern immediately via Safeguard/CPOMS.
- **PSHE / RSHE Lead (Ricky Sparham):** Embeds healthy digital relationships, consent, online harm prevention, and digital literacy into statutory RSHE modules.
- **Network Manager / Technical Support (Terry Carter / RM):** Manages dynamic web filtering and network monitoring tools (WebScreen 3, RM Buzz, DfE Umbrella, and LGfL's SENSO); maintains system security and backups; provides regular alert logs to the DSL team; and conducts technical system audits.
- **Data Protection Officer (Mira Gohil):** Ensures GDPR compliance; audits cloud platforms; and verifies that data protection rules never obstruct essential safeguarding information sharing.
- **Pupils & Parents/Carers:** Co-sign and uphold age-appropriate AUPs; enforce positive digital habits at home; and report suspicious or upsetting online encounters immediately.

Education and curriculum

Online safety is delivered across statutory RSHE, Computing, Citizenship, and cross-curricular learning. Schemes of work are adapted for SEND and vulnerable cohorts using contextual visual tools and targeted workshops (e.g., *SHINE*). Key topics include digital identity, healthy online relationships, critical thinking (fake news/AI awareness), managing privacy, and avoiding commercial exploitation.

Handling online-safety concerns and incidents

Workflow Escalation:

1. **Immediate Intervention & Preservation:** Secure pupil physical/emotional safety. Secure evidence (screenshots, URLs, logs). **Staff must NEVER view, copy, print, store, or forward illicit/sexual images of minors.**
2. **CPOMS / Safeguard Logging:** Log the factual incident immediately on Safeguard/CPOMS for DSL evaluation.
3. **DSL Triage:** Assess harm against local threshold frameworks. Low-level breaches are

addressed via restorative behavioral interventions. Severe harms (CSAE, CCE, grooming, sextortion) trigger immediate referrals to Children's Social Care (MASH) and Police. Allegations against staff are referred directly to the Headteacher and LADO within 24 hours.

Sharing Nudes and Semi-Nudes

Staff encountering incidents of youth-produced sexual imagery must notify the DSL immediately without capturing or transmitting the material. The DSL will apply UKCIS *Sharing Nudes and Semi-Nudes* guidance to evaluate consent, age differentials, coercion, and distribution risk, prioritizing safeguarding support over criminalization.

Generative AI, Deepfakes, and Sextortion

- **Legal Mandate:** Creating, possessing, or distributing AI-generated CSAM or non-consensual sexual imagery (deepfakes/nudification) is illegal in the UK and treated as a severe child protection issue.
- **Sextortion Protocol:** Incidents involving financial sexual extortion trigger immediate emergency intervention, evidence collection, DSL triage, and Police/CEOP escalation.
- **AI Tool Integrity:** Synthetic content produced to harass, bully, or defraud will result in device access revocation and formal disciplinary action.

Priority Areas

Online safety concerns and network misuse are flagged automatically through network filters and monitoring software, including RM Buzz, RM SafetyNet, and LGfL's SENSO. Any inappropriate use of technology or high-risk keyword detection is flagged instantly and routed to the Online-Safety Lead and DSL team to be investigated through standard safeguarding procedures on Safeguard/CPOMS.

- **Upskirting:** Recognized as a serious criminal offense; managed via immediate safeguarding escalation.
- **Cyberbullying:** Managed under the Anti-Bullying Policy, incorporating restorative support, targeted re-education, and platform takedown requests via POSH.
- **Sexual Violence & Harassment:** Handled with a zero-tolerance approach under DfE guidance. Low-level sexualized online behavior is challenged immediately to prevent normalization.

Cyber Security and Data Protection

Newham PRUs complies with DfE Cyber Security Standards and UK GDPR. Systems are secured using encrypted end-to-end cloud platforms, USO authentication, Sophos antivirus defenses, and multi-factor authentication for staff access.

Statutory Data Sharing Rule: UK GDPR and the Data Protection Act 2018 do not restrict the sharing of confidential information for child protection purposes. Missing consent must never prevent or delay a safeguarding referral where a child is at risk of harm.

Appropriate Filtering and Monitoring

In accordance with KCSIE 2026 mandates:

- **Filtering Controls:** On-site networks utilize LGfL WebScreen 3 alongside LGfL's SENSO software to inspect dynamic web content, search queries, and real-time activity. Remote Chromebooks and outreach devices are locked to the school domain and filtered via RM Buzz, SENSO, and DfE Umbrella. Dynamic inspection blocks inappropriate AI output, extreme content, and unsafe platforms while preventing over-blocking of academic or mental health support sites.
- **Monitoring Systems:** RM SafetyNet and LGfL's SENSO actively log search anomalies, keyword breaches, and device activities across all school endpoints, dispatching automated priority alerts directly to the DSL team and Online-Safety Lead (Luis Cravioto) for immediate triage.
- **Annual Audit Requirement:** The SLT, DSL, and Network Manager must execute and document a formal review of technical filtering and active monitoring efficacy (including SENSO configuration settings and alert thresholds) at least once per academic year.

Electronic Communications and Cloud Platforms

- **Email & Workspace:** Staff and pupils must exclusively use managed Google Workspace `@prus.newham.sch.uk` accounts. Private email addresses or unapproved communication tools are strictly prohibited.
- **Data Security:** Sensitive pupil data must be transmitted externally via encrypted channels (e.g., Egress).
- **Cloud Principles:** Access rights are strictly managed; administrative privileges are audited; and two-factor authentication is mandatory for staff access.

Digital Images, Video, and Social Media

- **Media Consent:** Media capturing requires written parental consent captured during admission. Published media uses first names only and excludes identify-revealing filenames or metadata.
- **Social Media Conduct:** Staff must maintain high professional boundaries, maximize privacy controls, and refrain from engaging with pupils or referencing school operational matters on private social media.
- **Pupil Restrictions:** Pupils are prohibited from requesting or adding staff members on personal social media accounts.

Device Usage and Mobile Phones

- **Default Mobile-Free Provision:** Pupils are strictly prohibited from possessing mobile phones or smart wearables during the school day. Devices must be surrendered upon arrival during morning entry search procedures and stored in locked security containers.
- **Staff Phone Etiquette:** Staff must keep personal devices on silent and out of sight when supervising or teaching children, restricting usage to designated adult-only areas.
- **Outreach / DRMO Devices:** School-issued Chromebooks remain strictly restricted to educational applications; home Wi-Fi access is dynamically monitored and filtered.

Searching and Confiscation

Authorised staff hold statutory powers under DfE *Searching, Screening and Confiscation* guidance to search pupils and their personal belongings. If staff reasonably suspect a device contains illegal, explicit, or harmful material, the device will be confiscated and handed immediately to the Headteacher or DSL for evidence review and potential law enforcement escalation.

Appendices

1. Safeguarding Incident Reporting Procedure: Logged centrally via Safeguard / CPOMS Portal
2. Child Protection & Safeguarding Policy: Available on the Newham PRUs Website
3. Behaviour Policy & Anti-Bullying Policy: Available on the Newham PRUs Website
4. Staff Code of Conduct / Handbook: Hosted on the internal Staff Google Drive
5. Staff Acceptable Use Policy (AUP) for Technology & AI
6. Parent / Carer Acceptable Use Policy Agreement
7. Pupil Acceptable Use Policy Agreement
8. DfE Guidance: Searching, Screening and Confiscation Advice for Schools
9. DfE & UKCIS Guidance: Sharing Nudes and Semi-Nudes: Advice for Education Settings

Newham PRUs – Acceptable Use Policy (AUP)

Parent / Carer Agreement

Context & Purpose

Digital technology supports learning at Newham PRUs. To protect pupils from digital harms—including online exploitation, cyberbullying, exposure to harmful content, and inappropriate interactions—we require parents/carers to sign this agreement annually.

Parent / Carer Commitments:

- **Technology & Monitoring:** I understand Newham PRUs uses managed devices and Google Workspace protected by filtering and monitoring systems (WebScreen 3, RM SafetyNet, DfE Umbrella, and LGfL's SENSO) to ensure safety.
- **Remote Learning Space:** I will provide a safe, quiet space for remote/outreach sessions. My child will be fully dressed, in a shared room where possible (not in bed), with video backgrounds blurred or neutral.
- **Social Media Conduct:** I will model positive online behavior and will not post disrespectful or defamatory comments about staff, governors, pupils, or parents online. Concerns will be raised via official school channels.
- **Media & Privacy:** I will respect data protection laws and will not record, screenshot, or share photos/videos of staff or pupils without written permission.
- **Emerging Online Risks:** I acknowledge the legal and safeguarding risks of Generative AI, deepfakes, nudification apps, and sextortion. Generating or sharing synthetic sexual imagery of minors is illegal. I will report any concerns to the school immediately.
- **Mobile & Devices:** I support the school's default mobile-free policy and understand student devices are collected during morning entry. I will ensure school Chromebooks are used strictly for educational work.

I agree to the terms outlined in this Acceptable Use Policy.

Parent/Guardian Signature: _____ **Date:** _____

Parent/Guardian Name (Printed): _____

Pupil Name: _____

Pupil Agreement

Context & Purpose

Computers and Chromebooks are provided for learning. These rules exist to keep you safe, protect your well-being, and ensure everyone is treated with respect.

My Rules for Using Technology:

- **Login & Passwords:** I will only access devices using my own login details. I will keep my passwords private, log out after use, and never access another user's files.
- **Online Behavior:** I will treat staff and pupils with respect. I will not use rude, aggressive, or hateful language in emails, Google Classroom, or shared files. Cyberbullying will not be tolerated.
- **Device Care & Filtering:** I will care for all school equipment. I will use the internet for schoolwork as directed and will never try to bypass school filtering or monitoring.
- **Mobile Phones:** I will hand in my mobile phone, smartwatch, or smart devices every morning during entry searches. Devices will be stored securely and returned at home time.
- **Generative AI & Media:** I will only use AI tools when given permission by a teacher. I will **never** use AI to create fake images, deepfakes, or abusive content. Creating or sharing illegal or explicit images is against the law.
- **Privacy & Reporting:** I will keep personal details private and never agree to meet anyone met online. If I see anything upsetting or unsafe online, I will tell a staff member immediately.

I understand that school devices and internet use are actively monitored (WebScreen 3, RM SafetyNet, and LGfL's SENSO) to keep me safe. Breaking these rules may lead to loss of computer access and disciplinary action.

Pupil Signature: _____ **Date:** _____

Pupil Name (Printed): _____

School Representative Signature: _____ **Date:** _____