



Grandpont
Nursery School & Childcare

Online Safety Policy 2026 – 2028

Updated for Keeping Children Safe in Education 2026 and the EYFS statutory framework effective 1 September 2026

Contents

1. Purpose and scope
2. Legal and statutory framework
3. Principles and online-risk categories
4. Roles and responsibilities
5. Safe systems, filtering and monitoring
6. Mobile phones, cameras and imaging/sharing devices
7. Teaching children about online safety
8. Working with parents and carers
9. Cyberbullying, harmful content and child-on-child abuse
10. Generative artificial intelligence
11. Acceptable use and staff working away from the setting
12. Responding to concerns, incidents and misuse
13. Training
14. Monitoring, audit and review

Last reviewed	September 2026
Next review	September 2028

15. Links with other policies

Appendix A. EYFS Parent acceptable-use agreement

Appendix B. Staff/governor/volunteer/visitor acceptable-use declaration

Appendix C. Staff training self-audit

Appendix D. Online-safety incident log

Appendix E. 2026 amendment sources

Purpose and scope

Grandpont Nursery School and Childcare aims to protect children, staff, volunteers, governors, visitors and families from online harm; support safe, purposeful use of technology; and establish clear arrangements to identify, record, respond to and escalate concerns.

This policy applies to all school-owned or managed technology and networks, all internet-connected devices used on the premises or for school business, remote access, school communications, digital images and recordings, and relevant use of personal devices where that use affects children, staff or the school.

Because this is a maintained nursery school, the policy must be read with both KCSIE 2026 and section 3 of the EYFS statutory framework from 1 September 2026.

Legal and statutory framework

This policy has been prepared with regard to:

Keeping Children Safe in Education 2026 (Department for Education, effective 1 September 2026), especially paragraphs 162-180 and Annex C.

Statutory framework for the Early Years Foundation Stage: group and school-based providers (Department for Education, effective 1 September 2026), especially paragraphs 3.4-3.9, 3.31-3.34 and Annex C.

Working Together to Safeguard Children; Prevent duty guidance; and the local safeguarding-partner procedures.

Data Protection Act 2018, UK GDPR and Data (Use and Access) Act 2025.

Education Act 1996; Education and Inspections Act 2006; Education Act 2011; Equality Act 2010; Human Rights Act 1998; and relevant statutory guidance on searching, screening and confiscation.

DfE Filtering and Monitoring Standards for Schools and Colleges; Cyber Security Standards for Schools and Colleges; Generative AI in Education; and Generative AI Product Safety Expectations.

Last reviewed	September 2026
Next review	September 2028

Principles and online-risk categories

Online safety is a running and interrelated theme across safeguarding, curriculum, staff training, parental engagement and the work of the DSL. Decisions will be child-centred, proportionate to the ages and needs of children, and attentive to children who may be at greater risk of harm.

The school addresses the four categories of online risk:

Content: illegal, inappropriate or harmful material, including pornography, racism, misogyny, self-harm, suicide, antisemitism, radicalisation, extremism, extreme sexual or physical violence, misinformation, disinformation and conspiracy theories.

Contact: harmful interaction with other users or generative-AI applications that simulate interaction, including grooming, exploitation, coercion, peer pressure and inappropriate advertising.

Conduct: online behaviour that causes or increases harm, including online bullying and making, sending or receiving explicit images, including images generated or altered using AI.

Commerce: online gambling, inappropriate advertising, phishing, financial scams and manipulative in-app purchasing.

Roles and responsibilities

4.1 Governing body

Approve this policy, hold the Executive Headteacher and Head of School to account and review online safety as part of the whole-school safeguarding approach.

Ensure all staff receive safeguarding training, including online safety and their filtering and monitoring responsibilities, at induction and through regular updates.

Ensure a senior leader is assigned responsibility for filtering and monitoring, supported by the DSL and IT support.

Ensure an effectiveness review is completed at least once each academic year, covers every internet-connected device in every relevant location, and is recorded.

Ensure children do not have access to mobile phones during the school day.

Receive sufficient information to test whether controls are effective, proportionate and do not unreasonably restrict teaching and learning.

Named safeguarding governor: Taryn Grant

Last reviewed	September 2026
Next review	September 2028

4.2 Executive Headteacher and Head of School

Ensure this policy is implemented consistently and resourced appropriately.

Approve exceptions and risk assessments relating to devices, systems and generative AI.

Ensure incidents that may constitute misconduct are handled under the Staff Code of Conduct and disciplinary procedures.

Executive Headteacher: Natalie Wilson

4.3 Designated Safeguarding Lead

Take lead responsibility for online safety and respond to safeguarding concerns identified through filtering, monitoring, disclosures or incidents.

Work with the responsible senior leader and IT support on filtering and monitoring reviews, risk assessment and escalation.

Maintain or oversee secure records of concerns, decisions, referrals and reasons for decisions.

Ensure staff understand safe handling of suspected illegal images: staff must not search for, copy, forward or routinely view such material and must report immediately.

DSL and deputies: Sarah Mason, DSL. Claire Thomas, Kulsum Faisal & Natalie Wilson DDSL.

4.4 Senior leader responsible for filtering and monitoring

Lead the at-least-annual effectiveness review with the DSL and IT support.

Check that filtering operates appropriately on all internet-connected devices in all relevant locations, including staff, visitor and curriculum networks where applicable.

Keep a dated record of tests, findings, actions, exceptions and follow-up checks.

Ensure relevant staff know the controls, their responsibilities and how to report a failure or concern.

Responsible senior leader: Rachel Duncalfe | IT support/provider: Koala IT, Phil Whicker

4.5 All staff, agency staff, contractors and volunteers

Read, understand and follow this policy and the applicable acceptable-use declaration.

Maintain professional curiosity, report concerns promptly to the DSL and never assume someone else will act.

Know how to report filtering or monitoring failures and never bypass controls unless specifically authorised for an approved purpose.

Last reviewed	September 2026
Next review	September 2028

Use only approved systems and devices for children’s information, images and recordings.

Report low-level concerns, allegations and unsafe practice through the school’s safeguarding and whistleblowing routes.

4.6 Parents, carers, visitors and community users

Parents and carers are asked to support age-appropriate safe use, discuss concerns with the school, follow the acceptable-use agreement and comply with device/photography rules on the premises. Visitors and

community users must follow the school’s acceptable-use and device instructions.

Safe systems, filtering and monitoring

The school will use age-appropriate filtering and monitoring on school devices and networks. Controls will block harmful and inappropriate content without unreasonably restricting education.

The school will identify and document the people responsible for technical controls, safeguarding response, review and escalation.

At least once each academic year, the responsible senior leader, supported by the DSL and IT support, will test effectiveness on all internet-connected devices in all relevant locations and keep a record.

Checks will include, as applicable, wired and wireless networks, curriculum devices, staff devices, shared devices, interactive screens, tablets, remote access, guest access and systems capable of accessing generative AI.

The school will record known limitations, authorised exceptions, actions, owners and completion dates. Urgent failures will be escalated immediately and children’s access restricted until risk is controlled.

Monitoring will be proportionate, transparent and handled in line with data-protection law. Access to monitoring data will be restricted to authorised personnel.

Information security

The school will protect personal information and maintain cyber-security measures consistent with DfE standards, including secure access management, supported and patched systems, backups, incident response and staff awareness. Suspected personal-data breaches will be reported immediately to the data protection lead.

Data protection lead/DPO and breach route: Phil Whicker, Koala IT

Last reviewed	September 2026
Next review	September 2028

Mobile phones, cameras and imaging/sharing devices

Children's devices

The school is mobile-phone-free for children by default. Children must not access a mobile phone or other personal connected device during the school day. Any exception must be authorised by the Executive Headteacher, be necessary for an individual child, and be supported by a written risk-managed arrangement shared with relevant staff and the parent/carer.

Staff, visitors and volunteers

Personal mobile phones, smart watches, cameras and other devices with imaging or sharing capability must be stored and used only as specified in the school's Mobile Phone and Smart Device Policy.

Personal devices must never be used to photograph, film or record a child, access a child's record, or communicate with a child or family on behalf of the school.

Images or recordings of children may be created only for an approved purpose, using an approved school device and approved account/storage, with appropriate consent or other lawful basis and in accordance with retention arrangements.

No image or recording may be copied to personal storage, personal messaging, personal email, social media or an unapproved cloud/AI service.

Visitors must be informed of the restrictions. Any suspected breach must be reported immediately to the DSL and may be treated as a safeguarding concern, low-level concern, allegation or data breach as appropriate.

Teaching children about online safety

Children will learn through play, stories, modelling, conversation and carefully supervised use of technology. Teaching will rarely include technology but when used will be appropriate to each child's age, development, communication and SEND needs and will include:

asking a trusted adult before using a device or going online;

recognising that not everything seen or heard on a screen is reliable or kind;

keeping names, images and other personal information private;

using technology kindly and respectfully;

stopping and telling a trusted adult if something is confusing, frightening, upsetting or unexpected;

Last reviewed	September 2026
Next review	September 2028

understanding that adults help choose safe content and that school devices have safety controls.

Technology use will be supervised and purposeful. Staff will not rely on a child independently using any device.

Working with parents and carers

The policy will be available to parents and carers, and concerns may be raised with any member of staff, the Executive Headteacher, Head of School or DSL.

The school will explain, in proportionate terms, how school devices and networks are filtered and monitored, what children may be asked to access online, and who from the school may interact with them online.

The school will share age-appropriate guidance on devices, images, privacy, online content, parental controls and reporting concerns, and will respond to emerging risks affecting the community.

School contact for online-safety queries: Rachel Duncalfe – 01865 242900 and Phil Whicker – 01865 634240

Cyberbullying, harmful content and child-on-child abuse

Online harmful behaviour may occur even in relation to very young children through family devices, messaging, images, games or content. Staff will respond to the impact and safeguarding context rather than dismissing behaviour because of a child's age.

All child-on-child abuse, harassment or violence is a safeguarding concern for the child harmed and may also indicate unmet need or risk affecting the child whose behaviour caused harm. It is preventable and will not be treated as banter or an inevitable part of growing up.

The DSL will coordinate support, risk assessment, recording, parental communication and referral where appropriate. Staff must preserve potential evidence without forwarding, copying or unnecessarily viewing harmful or suspected illegal material.

Generative artificial intelligence

No child will use a generative-AI service unless it is approved, age-appropriate, directly supervised and covered by a proportionate risk and data-protection assessment.

Staff must follow service age limits and terms, use approved accounts and maintain human oversight of all outputs.

Identifiable or special-category information about a child, family or member of staff must not be entered into a public or unapproved generative-AI service.

AI output may be inaccurate, biased, inappropriate or manipulative. Staff must check outputs before using them and must not use AI as the sole basis for safeguarding, assessment, admission, employment or other significant decisions.

Last reviewed	September 2026
Next review	September 2028

AI systems capable of simulated interaction, image creation or alteration are included in the school's content, contact, conduct and filtering/monitoring risk assessments.

AI-generated or altered sexual images of a child are safeguarding concerns and may be illegal. They must be reported immediately to the DSL and handled without copying, forwarding or unnecessary viewing.

Acceptable use and staff working away from the setting

School systems and internet access are for approved educational or work purposes. Users must follow the applicable acceptable-use declaration. The school may monitor use lawfully and proportionately to protect children, people, systems and information.

Work devices must be password protected, encrypted where supported, locked when unattended, kept patched and protected, and not shared with family or friends.

School information must be accessed and stored only through approved accounts and systems; work must not be forwarded to personal email or copied to unapproved storage.

Staff must protect screens and conversations from unauthorised viewing when working away from the setting and report loss, theft, suspicious access or a data breach immediately.

Responding to concerns, incidents and misuse

Ensure immediate safety; do not investigate beyond what is necessary to establish and report the concern.

Report safeguarding concerns immediately using CPOMS and to the DSL or deputy. If they are unavailable and a child may be at risk, follow the Child Protection and Safeguarding Policy and local referral procedures without delay.

Do not promise confidentiality. Record facts, the child's words where relevant, actions, decisions and rationale promptly in the approved system.

Do not search for, copy, forward, print, save or unnecessarily view suspected illegal child sexual abuse material or nudes/semi-nudes. Isolate the device where safe and seek DSL/police advice.

Consider whether the matter is also a filtering failure, cyber incident, personal-data breach, low-level concern, allegation, disciplinary matter or criminal offence, and activate the relevant procedure.

Where a concern relates to the Executive Headteacher, report it using the allegation procedure to the chair of governors and/or LADO route specified in the Child Protection and Safeguarding Policy.

Safeguarding recording system: CPOMS

Last reviewed	September 2026
Next review	September 2028

Emergency/out-of-hours route: If you think a child is in immediate danger, call the police on 999

MASH on 0345 050 7666 during office hours (8.30am – 5pm, Monday to Thursday, 8.30am – 4pm, Friday)

Outside office hours call the Emergency Duty Team on 0800 833 408

LADO route: If you are a practitioner and have concerns about another practitioner or volunteer who works with children, or you need to report them, you will need to contact the Local Authority Designated Officer (LADO) on 01865 810603

Data-breach route: DPO – Phil Whicker, Koala IT – 01865 634240

Training

All practitioners will receive safeguarding training meeting the EYFS 2026 Annex C criteria. Training will be appropriate to children aged 0-5, include the setting's procedures and internet safety, and support practitioners to put the policy into practice. Training must be renewed every two years; the school will also provide regular updates and consider annual refresher training where needed.

KCSIE also expects safeguarding and child-protection updates, including online safety, as required and at least annually. Staff working directly with children, and from September 2026 staff not working directly with children, are expected to read Part One of KCSIE in full.

The DSL must receive appropriate DSL training at least every two years and maintain knowledge and skills through regular, at least annual, updates. Governors will receive role-appropriate safeguarding and online-safety training.

Training record location: Safesmart, online

Monitoring, audit and review

The DSL will monitor safeguarding and behaviour concerns relating to online safety and report themes to the Executive Headteacher, Head of School and governing body without disclosing unnecessary personal information.

The school will complete an annual online-safety risk assessment and policy review, alongside the filtering and monitoring effectiveness review.

Review will consider children's ages and needs, emerging technology, AI, incidents, near misses, staff confidence, parental feedback, filtering data, local safeguarding intelligence and changes to statutory guidance.

The policy will also be reviewed after a serious incident, significant system change or relevant statutory change.

15. Links with other policies

Last reviewed	September 2026
Next review	September 2028

- Child Protection and Safeguarding Policy
- Mobile Phone and Smart Device Policy
- Staff Code of Conduct
- Behaviour, Relationships and Emotional Health Policy
- Data Protection Policy and privacy notices
- Whistleblowing Policy
- Complaints Procedure

Appendix A. Parent/carers agreement

I give permission for my child to use approved school technology under appropriate supervision. I will support the simple rules above and contact the school if I have a concern. I understand that school devices and networks use filtering and monitoring to help keep children safe.

Parent/carers name: _____ Signature: _____ Date: _____

Appendix B. Staff/governor/volunteer/visitor acceptable-use declaration

I will use approved accounts, systems, networks and devices only for authorised purposes.

I will keep passwords and access methods secure and use multi-factor authentication where provided.

I will not use a personal device to photograph, record or store information about a child.

I will not enter identifiable or sensitive school information into an unapproved AI or cloud service.

I will not disable or bypass filtering, monitoring or security controls unless specifically authorised for a documented purpose.

I will report online-safety concerns, filtering failures, loss/theft, suspicious access, accidental disclosure and other incidents immediately through the stated route.

I understand that authorised, lawful and proportionate monitoring may take place and that misuse may result in safeguarding, disciplinary, contractual, civil or criminal action.

Last reviewed	September 2026
Next review	September 2028

Name: _____ Role: _____ Signature: _____
 Date: _____

Appendix C. Staff training self-audit

Confirmation of below statements implied when confirmation of reading policy given. If staff do not know the answer to any of the statements, it is their responsibility to speak to a DSL to ask.

Statement	Yes / No	Action or training needed
I know who the DSL/deputies and filtering/monitoring lead are.		
I know how to report a safeguarding concern and a filtering/monitoring failure.		
I understand the four online-risk categories, including AI-related risks.		
I understand the rules for personal devices, cameras, images and sharing-capable devices.		
I know how to respond without copying, forwarding or unnecessarily viewing suspected illegal imagery.		
I know which systems, storage and AI tools are approved.		
I know the data-breach and cyber-incident reporting routes.		
I can adapt online-safety support for children aged 0-5 and individual SEND/communication needs.		

Appendix D. Online-safety incident log

Date/time	Child/system/location	Facts and risk	Immediate action	Referrals/notifications	Outcome/review

Last reviewed	September 2026
Next review	September 2028

Do not duplicate sensitive detail unnecessarily. The safeguarding record is the authoritative record where the incident concerns a child.

Appendix E. 2026 Primary sources

Department for Education, Keeping Children Safe in Education 2026:

https://assets.publishing.service.gov.uk/media/6a4cf903b7203c4c023fd2f3/Keeping_children_safe_in_education_2026_.pdf

Department for Education, Statutory framework for the Early Years Foundation Stage: group and school-based providers, effective 1 September 2026:

https://assets.publishing.service.gov.uk/media/6a5f8e4fb00f3323bf1a23a1/EYFS_group_and_school_based_from_September_2026.pdf

Grandpont Nursery School and Childcare, Online Safety Policy 2024-2025 (website resource recovered 4 August 2026):

https://www.grandpontnurseryschool.co.uk/goto/601864?slug=policies_procedures_and_statutory_reports

Department for Education, Meeting digital and technology standards in schools and colleges (Filtering and Monitoring; Cyber Security): <https://www.gov.uk/guidance/meeting-digital-and-technology-standards-in-schools-and-colleges>

Department for Education, Generative artificial intelligence in education:

<https://www.gov.uk/government/publications/generative-artificial-intelligence-in-education>

Department for Education, Mobile phones in schools:

<https://www.gov.uk/government/publications/mobile-phones-in-schools>

Last reviewed	September 2026
Next review	September 2028