Chertsey and Dorking Nursery Schools

ONLINE SAFETY POLICY

1. Policy Statement & Aims

Online safety is an integral part of our safeguarding duty to protect children from harm, including risks arising from the use of digital technology.
This policy applies to all staff, volunteers, governors, visitors, contractors, parents/carers and children within our setting.

Aims

- To ensure all staff adopt safe practices in the use of the Internet and understand about acceptable use.
- To begin to educate children and parents to be responsible and informed technology users.
- To ensure that online safety is an integral part of our commitment to safeguarding children and relates to other policies.
- To ensure that requirements from Keeping Children Safe in Education (2025) are reflected in our practice and policy.
- To ensure all staff understand how to protect children from maltreatment, whether that is within or outside the home, including online.
- To establish clear roles, responsibilities and governance for online safety, including oversight by the governing body.
- To define acceptable use for identified staff through signed Acceptable Use Agreements (AUPs).
- To ensure robust filtering and monitoring is in place, reviewed, and effective for our age range.
- To set out a clear incident reporting and escalation procedure, including liaison with external agencies where appropriate.
- To promote safe, responsible and respectful use of technology through the EYFS curriculum and partnership with parents/carers.

2. Roles & Responsibilities

The following roles have specific responsibilities for online safety across the setting:

Governing Body

- Hold strategic oversight of online safety and seek assurance that risks are identified, managed and reduced.
- Review filtering and monitoring arrangements at least annually with the Designated Safeguarding Lead.
- Approve this policy and monitor its implementation.

Executive Headteacher/ Leadership Team

- Ensure online safety is embedded across safeguarding, curriculum, data protection and staff development.
- Allocate resources and support the DSL to discharge their duties effectively.
- Promote a culture of safe and responsible technology use.

Designated Safeguarding Lead (DSL) and Deputies

- Lead on online safety, including responding to concerns, recording, and liaising with external agencies as required.
- Oversee and regularly review filtering and monitoring reports; investigate and act on incidents.
- Ensure staff receive induction and regular updates in online safety; provide advice and guidance.

All Staff and Volunteers
- Read and follow this policy and the relevant AUP; complete required training.
- Promote children's use of any digital technology and promote safe behaviours.
- Report online safety concerns immediately to the DSL.

IT Support/Service Providers
- Implement and maintain technical controls (e.g. filtering, monitoring, antivirus, updates).
- Provide reports to the DSL and support incident response and evidence preservation as required.

Parents/Carers
- Support safe technology use at home and the setting's guidance on sharing images.
- Use official communication channels for enquiries and concerns.

3. Acceptable Use Agreement (AUPs) Policies
The setting uses AUPs policies and procedures for staff and governors. Signed AUPs are a condition of access to the setting's systems and platforms for identified staff using school owned devices.
A summary of expectations is below; AUP for devices is provided in the Appendix.

Staff /Governor AUP (summary)
- Use only work accounts and devices for work-related communication; keep credentials secure and use MFA where provided.
- Do not install unauthorised software/hardware or use personal cloud storage/USB devices for work data.
- Never share personal contact details with parents/carers; maintain professional boundaries online.
- Use images and recordings only with consent and in line with policy; store only on approved systems.

Parent/Carer AUP (summary)
- Use images of your own child only; do not share images of other children on social media or messaging apps.
- Seek permission to take photographs and images at school events and follow the guidance accordingly.
- Use Tapestry to share images with key people.
- Use the setting's communication platforms respectfully and for appropriate purposes.
- Raise concerns through official channels rather than on social media.

Volunteer/Visitor AUP (summary)
- Follow staff instructions; no use of personal devices for photography or recording.
- Report any online safety concern to a member of staff/DSL immediately.

4. Curriculum: Teaching Online Safety in EYFS
Online safety is taught through the EYFS prime and specific areas (especially Personal, Social and Emotional Development and Understanding the World). We may use stories, role-play and discussions to develop early digital resilience.
- Key messages include: asking a trusted adult for help; being kind; keeping information private; and understanding that photos and videos are special and need permission.
- Staff model safe use of technology and use age-appropriate resources.

5. Devices, Filtering & Monitoring
Children across our organisation do not have access to technology connected to the internet whilst at nursery. The IT systems are configured to restrict access to those who require it. The network is password-controlled and protected by anti-virus under IT support contracts.

- Laptops and tablets are issued to some staff depending on their role; devices used off site must not be left unattended and must be password protected.
- Memory sticks and other portable devices are not to be used at any time; documents must be stored on the secure network or Office 365 cloud only.

There are filtering and monitoring systems in place for all users; inappropriate access attempts are blocked and reported. Daily reports are provided to the lead DSL on each site and followed up.
Our filtering and monitoring arrangements are reviewed at least annually or after any significant change, to ensure effectiveness for our age range and to minimise impact on teaching and learning.

- Specific roles and responsibilities for managing filtering/monitoring are assigned and documented.
- Staff are informed about the systems in place and how to escalate concerns.
- Filtering operates across all setting-managed devices, including tablets used for observations.
- Filtering also operates for any users on the Staff and Guest Wi-fi.

6. Images, Media Recording & Data Protection
Parental permission is obtained before using images of children on websites or social media. Children are not named alongside images. We rotate images in line with data retention considerations.
Tapestry (online learning journal) is used with password-protected access for parents to their own child and tiered staff access according to role. Tablets used for Tapestry are PIN-protected and monitored.
We handle personal data in line with UK GDPR and our Data Protection Policy, including data minimisation, secure storage, access control, and retention/disposal schedules. Data Protection Impact Assessments (DPIAs) are completed for new or significantly changed platforms or processes.

- We only use third-party platforms that meet our data protection standards and have appropriate agreements in place.
- Staff must not transfer personal data to personal devices or unapproved services.

7. Smart Devices & Mobile Technologies
Mobile telephones are kept in staff areas and are not to be taken into the classrooms by staff in ratio, as per the Safeguarding Policy. There may be occasions, at the discretion of the Headteacher, whereby for H&S premises evidence an image must be taken by the Business Manager or other using their mobile phone.
Staff are permitted to wear smart watches as long as these are used for time-telling purposes only and connected devices are not transferring a signal/messages during teaching time when staff are in classrooms.
The following procedures apply to smart technologies to safeguard children and staff:

- Children: No personal mobile phones or smart devices are permitted on site.
- Staff: Personal phones must remain in lockers/staff areas; no photography/recording on personal devices.
- Visitors/Contractors: Personal devices must not be used in learning areas; no photography/recording. Visitors are briefed on arrival and supervised as appropriate.
- Parents/Carers at events: Filming/photography is permitted for personal use of your own child only; images of other children must not be shared online without consent.

8. Staff Conduct & Social Media
Staff should be aware that content on social networking websites may be detrimental to their professional image, this includes messaging apps. Staff must not communicate with parents/carers or children via personal social media accounts; they must not share confidential information or images related to the setting on personal platforms.

- Only nominated staff may post on official setting accounts; posts must use consented images and protect confidentiality.

- Staff must maintain professional tone and boundaries online and report any contact attempts from parents/carers via personal channels.

9. Incident Reporting & Escalation
All online safety concerns must be reported immediately to the DSL. The DSL will log, investigate, take proportionate action and record outcomes.
- If a child is at immediate risk of harm, staff will inform the DSL without delay; the DSL may contact children's services or the police.
- Allegations about staff are managed under the Safeguarding/Allegations policy and may require consultation with the LADO.
- Where illegal content or activity is suspected, the DSL will preserve evidence, avoid further access, and seek advice from police and relevant agencies.
- Parents/carers will be informed where appropriate, considering the safety and privacy of the child.

10. Parent/Carer Engagement
We work in partnership with parents/carers to promote safe use of technology at home and at nursery.
- Regular updates via newsletters and the website/app with tips and current themes.
- Clear guidance on sharing images responsibly and on expected conduct within communication platforms.

11. Cyberbullying & Online Behaviour
The setting does not permit bullying or harassment in any form, including online behaviours between adults or involving the community. Any incidents will be addressed under our Behaviour and Safeguarding policies.
- Examples include: sharing unkind content about staff/parents online; misuse of messaging groups; posting images without consent.
- The DSL will assess impact, take action to stop harm, support those affected, and record actions/outcomes.

12. Risk Assessment & Review
An annual online safety risk assessment is conducted to identify and mitigate risks relating to people, processes and technology. Findings inform training, technical controls and policy updates.
- Filtering and monitoring reviews are documented with actions, owners and target dates.
- This policy is reviewed at least annually, or sooner following significant changes or incidents.

13. Linked Policies
This policy should be read alongside the following related policies:
- Safeguarding & Child Protection Policy
- Staff Behaviour (Code of Conduct) Policy
- Behaviour Policy
- Data ProtectionPolicy
- Complaints Policy
- Whistleblowing Policy

Approved by the Governing Body: March 2026
To be reviewed by: March 2027
Relevant for:-

Nursery: Yes	**Parents**: Yes

Appendix A: Acceptable Use Agreement for Devices

Chertsey and Dorking Nursery Schools
Acceptable Use Agreement (AUA) for Work-Owned Devices

This Acceptable Use Agreement (the 'Agreement') sets out the conditions under which staff may use work-owned device devices (the 'Device') provided by the school.
By signing, you confirm that you have read, understood, and agree to comply with this Agreement and related policies.

1) Purpose & Scope
This Agreement applies to all staff who are issued a work-owned device for the purposes of teaching and learning practices. It covers use on and off site, during and outside working hours.

2) Roles & Responsibilities
- You must use the Device only for legitimate school purposes. Under no circumstances is it to be used for personal use.
- You are responsible for the physical security and safe return of the Device, including accessories, and any removable media.
- By signing this agreement, you accept that the device is issued in workable condition, with screen protector, device case, charger lead and carry strap. If any items are lost or damaged, you may be responsible for the costs.
- If at any time the device, case or screen protector is damaged, this must be reported immediately for replacement, otherwise you will be responsible for the costs. For example if the device is dropped which results in a smashed screen, this will not be covered by the school if not in a protective case or with screen protector.
- You must follow all applicable policies (e.g., safeguarding/child protection, data protection, behaviour , Online Safety).

3) Safeguarding & Professional Conduct
- Only capture photos, videos, or audio of children when this is part of an authorised activity.
- Store and access child images or observations only within approved systems/apps. Do not save to personal cloud accounts or personal devices.
- Never use personal messaging or social media to communicate with children or parents/carers. Use approved channels only.
- Do not display or access inappropriate, offensive, or adult content. Maintain professional boundaries at all times.

4) Data Protection & Privacy
- Access personal data strictly on a need-to-know basis and only for legitimate school purposes.
- Use only approved, secure apps and systems for any processing of personal data (children, parents/carers, staff).
- Do not share your passcode.
- Do not copy personal data to unencrypted storage (including screenshots, downloads, external drives) or personal email/cloud accounts.
- Keep data no longer than necessary and follow retention and deletion procedures, you are responsible for deleting images from the camera roll once uploaded to Tapestry.

5) Device Security & Acceptable Use
- Do not attempt to jailbreak, root, or otherwise bypass security settings or mobile device management (MDM).
- Install apps only from the school's managed app store or with prior approval from the Head. Do not install personal or unlicensed software.
- Keep the operating system and apps up to date. Do not disable security updates or anti-malware where used.
- Do not connect the Device to unknown computers or charge from untrusted USB ports without a data blocker.
- Do not share the Device with children or unauthorised persons. Supervise the Device at all times around children.
- Use protective cases and maintain the Device in good condition. Report faults promptly; do not attempt unauthorised repairs.

- Understand that the device will be monitored by the schools filtering and monitoring systems.

6) Internet, Email & Communications
- Do not add work or other email account to the device. Outlook on this device is logged into and to be used for Emergency lockdown purposes only.

7) Monitoring & Privacy Notice
The School may monitor Device activity, location, and network traffic for security, safeguarding, and policy compliance, in accordance with applicable laws and provided privacy notices.

8) Loss, Theft & Incidents
- If the Device is lost, stolen, or compromised, report immediately to the Head and the DSL. The School may remotely lock or wipe the Device.
- Complete incident forms as required. Cooperate with investigations and safeguarding procedures.
- Devices should be stored in secure areas in the school in line with Online Safety policy and if removed from the site, are to be kept in possession of staff member at all times, not left in parked cars.

9) Leaving Employment or Role Change
- Return the Device and accessories on or before your last working day, or when requested.
- Ensure work data is synced to approved systems and remove any locally stored data under IT guidance.

10) Breaches & Consequences
Misuse or breach of this Agreement may result in disciplinary action, revocation of Device access, and, where applicable, reporting to regulatory or safeguarding authorities.

11) Related Policies & References
This Agreement should be read alongside the School policies on: Safeguarding/Child Protection, Staff Code of Conduct, Behaviour, e-Safety, Data Protection and Retention.

Acknowledgement & Signature
I confirm that I have read and understood this Agreement and agree to comply with its terms and all related policies. I understand that non-compliance may result in disciplinary action.

Device issued asset number:	
IMEI:	
IP address:	
Screen protector:	Yes/ No
Case:	Yes/ No
Strap	Yes/ No
Charging lead:	Yes/ No

Staff name (print):	
Role:	
Signature:	
Date:	
Manager/DSL (name & signature):	