E-Safety Policy

Camden

Thomas Coram Nursery School
49 Mecklenburgh Square
WC1N 2NY

Review and Approve: **Summer 2022**	**Next review:** **Summer 2024** Reviewed bi- annually

Policy Statement

As a school, we have a duty to ensure that children are protected from potential harm both within and beyond the learning environment. Every effort will be made to safeguard against all risks in regards to all technology. Any incidents that do arise will be dealt with quickly and according to policy to ensure that children and staff continue to be protected.

Aims

- To raise awareness amongst staff and parents/carers of the potential risks associated with online technologies, whilst also highlighting the many educational and social benefits.
- To provide safeguards and rules for acceptable use to guide all users in their online experiences.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the early years setting. Scope of policy

This policy applies to all staff, children, parents/carers, visitors and contractors accessing the internet or using technological devices on the premises. This includes the use of personal devices by all of the above mentioned groups, such as mobile phones or iPads/tablets which are brought into an early years setting. This policy is also applicable where staff or individuals have been provided with setting issued devices for use off-site, such as a work laptop or mobile phone.

The policy is reviewed bi- annually.

Responsibilities Practitioners (including volunteers)

All staff have a shared responsibility to ensure that children are able to use the internet and related technologies appropriately and safely as part of the wider duty of care to which all adults working with children are bound. Please see Thomas Coram Code of Conduct and Staff handbook for further details regarding staff responsibilities and expectations for behaviour whilst accessing the internet, email or related technologies within and beyond the early years setting. A copy of this policy should be made available to all staff and shared with any volunteers and students.

IT Department -The ICT Technician (Camden SITSS) is responsible for ensuring that:

- The setting's ICT infrastructure/system is secure and not open to misuse or malicious attack.
- Anti-virus software is installed and maintained on all setting machines and portable devices.
- The setting's filtering policy is applied and updated on a regular basis.
- Any problems or faults relating to filtering are reported to the ICT Technician immediately and recorded on the SITSS helpdesk.

• Users may only access the setting's network through a rigorously enforced password protection policy, in which passwords are regularly changed.

• The admin team and relevant staff keep up to date with e safety technical information in order to maintain the security of the network and safeguard children.

• Any deliberate or accidental misuse MUST be reported to the Designated Safeguarding Officer (Perina Holness).

Broadband and Age Appropriate Filtering

We use internet enabled devices, including iPad educational apps and games, to enhance the learning experience of children. For this reason, great care must be taken to ensure that safe and secure internet access, appropriate for both adults and children, is maintained with all staff being responsible for reporting any problems.

• Filtering levels are managed and monitored on site via an administration tool/control panel, provided by our broadband supplier, which allows authorised IT technicians to instantly allow or block access to sites and manage user internet access.

• Age appropriate content filtering is in place across the setting, ensuring that staff and children receive different levels of filtered access in line with user requirements (e.g. Youtube blocked to children and not used 'live' with them due advert pop-ups etc.)

Email Use (staff)

• The setting provides all staff with access to a professional email account to use for all work related business, including communication with parents and carers. This allows for email content to be monitored and protects staff from the risk of allegations, malicious emails or inappropriate contact with children and their families. Personal emails will not be shared with parents/ carers.

• Staff must not engage in any personal communications (i.e. via hotmail or yahoo accounts etc) with children who they have a professional responsibility for. Contact with former pupils outside of authorised setting email channels is also prohibited.

• All emails should be professional in tone and checked carefully before sending, just as an official letter would be.

Use of Social Networking Sites is prohibited. Best practice guidance states that:

• To maintain professional distance and to avoid unwanted contact, staff should not link their personal social networking accounts to the schools web-page or 'friend' families who attend the school.

• Ensure that privacy settings are set to maximum and checked regularly.

• For safeguarding purposes, photographs or videos of any children at the school must not be shared on social networking sites.

Staff Mobile Phones:

• Personal mobile phones are permitted on setting grounds, but are to be used during break times only, within designated areas away from children i.e. the staff room, sensory room and the parents room if not in use by any parents or carers.

• Personal mobile phones must never be used to contact children or their families, nor should they be used to take videos or photographs of children. Photographs and Video Digital photographs and videos are an important part of the learning experience in early years settings and, as such staff have a responsibility to ensure that they not only educate children about the safe and appropriate use of digital imagery, but also model good practice themselves. To this end, there are strict policies and procedures for staff and children about the use of digital imagery and videos: School issued devices only should be used for this purpose and, if containing sensitive information or photographs of children, should not leave the premises unless encrypted

• At the point of admission, written consent is obtained from parents or carers before photographs or videos of young people will be taken or used within the setting, including displays, learning journeys, setting website and other marketing materials.

• Staff will ensure that children are at ease and comfortable with images and videos being taken.

• Staff must not use personal devices, such as cameras, video equipment or camera phones, to take photographs or videos of children.

Laptops/iPads/Tablets- Staff Use:

• A log of all ICT equipment issued to staff, including serial numbers, is maintained in the school's inventory.

• Where staff have been issued with a device (e.g. laptop) for work purposes, personal use whilst off site is not permitted unless authorised by the head teacher. The settings laptop/devices should be used by the authorised person only.

• Staff are aware that all activities carried out on setting devices and systems, both within and outside of the work environment, will be monitored in accordance with this policy.

• Staff will ensure that laptops and devices are made available as necessary for antivirus updates, software installations, patches, upgrades or routine monitoring/servicing.

• Please note: Senior Management is ultimately responsible for the security of any data or images held of children within the setting.

Laptops/iPads/Tablets- Children's Use:

• Laptop, iPad or tablet use must be supervised by an adult at all times and any games or apps used must be from a pre-approved selection checked and agreed.

• Online searching and installing/downloading of new programmes and applications is restricted to authorised staff members only. Children should not be able to search or install anything on a setting device. Data Storage and Security

• Sensitive data, photographs and videos of children are not stored on setting devices which leave the premises (e.g. laptops, mobile phones, iPads, USB Memory Sticks etc) unless encryption software is in place.

Parents, carers and visitors are not allowed to use mobile phones within the setting when with the children. Designated areas are made available.