POLICY No: SNP008.1

TITLE: E-SAFETY POLICY

VERSION: 02

VERSION	BREIF DECRIPTION OF CHANGE:	APPROVED BY:	EFFECTIVE DATE	REVIEW DATE
02	UPDATED TO REFLECT NEW EYFS CHANGES	TARA (NURSERY MANAGER)	DEC 2023	DEC 2024

E-Safety Policy

Legislation & Guidance

This policy has been drawn up on the basis of law and guidance that seeks to protect children, namely:

- Children Act 1989
- United Convention of the Rights of the Child 1991
- Data Protection Act 1998
- Freedom of information Act (2000)
- Sexual Offences Act 2003
- Serious Crime Act 2015
- Children Act 2004
- Keeping Children Safe in Education (2023)
- Working Together to Safeguarding Children (2023)

Scope of Policy:

This policy and the procedures that it underpins applies to all staff, children, parents/carers, committees, 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 Sunnyside Nursery. This policy is also applicable where staff or individuals have been provided with our nursery issued devices for use off-site, such as a work laptop or mobile phone. We endeavor to:

- Protect children who receive Sunnyside Nursery services and who make use of information technology as part of their involvement with us.
- Provide staff and volunteers with the overarching principles that guide our approach to e-safety.
- Ensure that, as an educator, we operate in line with our values and within the law in terms of how we use information technology.

Introduction

As more of our lives move online different opportunities, challenges and risks present themselves. Although, the web is a source of support, information and learning, unfortunately it is also a place of grooming, exploitation and bullying. Therefore, Sunnyside Nursery understands that we play a key role in supporting children to learn about how to stay safe online. Online Safety is not just an IT issue; it is about safeguarding children (and adults) in the digital world as part of our safeguarding responsibilities.

E-Safety Policy

At Sunnyside Nursery we will focus on building children's resilience to online risk so they can be safe and confident online. This often requires practitioners, parents and carers to build their own understanding of today's digital world.

E-safety encompasses not only internet technologies but also includes all electronic devices with imaging and sharing capabilities such as; mobile phones and wireless technology. Sunnyside Nursery's E-safety policy focuses on educating staff, children and their families about the benefits, risks and responsibilities of using information technology. Sunnyside Nursery believes effective e-safety provides safeguards and raises awareness to enable users to control their online experiences.

Our Aim

Children will experiment online, and while their confidence and enthusiasm for using new technologies may be high; their understanding of the opportunities and risks may be low, alongside their ability to respond to any risks they encounter. Therefore, we will:

- Decide on the right balance between controlling access, setting rules and educating children for responsible use.
- Offer valuable guidance and resources to staff to ensure that they can provide a safe and secure online environment for all children in their care.
- 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.
- Focus on utilising and embedding these technologies into the curriculum in order to model age appropriate, effective and safe use therefore empowering and equipping children with the skills and knowledge they need to use these technologies safely and responsibly, and managing the risks, wherever and whenever they go online.
- Use effective AUPs can help to establish, and reinforce, safe and responsible online behaviours.
- To ensure adults are clear about procedures for misuse of any technologies both within and beyond the early years setting.

Management Responsibilities

Tara Lougheed (Nursery Manager) and Shalina Miah (Deputy) manages the lead role of eSafety:

• Ensuring that the eSafety Policy and associated documents are up to date and reviewed regularly;

- Ensuring that the policy is implemented and that compliance is actively monitored;
- Ensuring that all staff are aware of reporting procedures and requirements should an eSafety incident occur;
- Ensuring that the eSafety incident log is appropriately maintained and reviewed regularly;
- Keeping up to date with eSafety issues and guidance through liaison with the School ICT Team;
- Ensuring eSafety updates, training and advice is available for staff, parents/carers and governors;
- Liaison with Senior Designated Person(s), that ensures a coordinated approach across relevant safeguarding issues.

Staff Responsibilities

All practitioners (including volunteers) have a shared responsibility that includes:

- 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.

Broadband and Age Appropriate Filtering

Broadband provision is essential to the running of an early years setting, not only allowing for communication with parents and carers but also providing access to a wealth of resources and support. Many settings now use internet enabled devices, including iPad educational apps and games, to enhance the learning experience of children or as online tools for staff to track and share achievement. For this reason, great care must be taken to ensure that safe and secure internet access, appropriate for both adults and children, is made available.

- Filtering levels are managed and monitored on behalf of the setting by Shalina

- Sunnyside Nursery 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.

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

- Email is covered by the Data Protection Act (1988) and the Freedom of information Act (2000) so safe practise should be followed in respect of record keeping and security.

- All staff are aware that all email communications may be monitored at any time in accordance with the 'Acceptable Use Policy'. All users must report immediately any email that makes them feel uncomfortable, is offensive, threating or bullying in nature.

Use of Social Networking Sites (advertising or parental contact)

Social networking sites (e.g. Facebook and X (formally known as Twitter) can be a useful advertising tool for early years settings and can often be an effective way of engaging with busy or hard to reach parents. Due to the public nature of social networking and the inability to keep content truly private, great care must be taken in the management and use of such sites. Best practice guidance states that:

- Identifiable images of children should not be used on social networking sites. Therefore, images of children's faces will be blurred to prevent identification and in all cases parental/carer consent will be obtained.

- To maintain professional distance and to avoid unwanted contact, staff should not link their personal social networking accounts to the setting's page.

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

- For safeguarding purposes, photographs or videos of looked after children must not be shared on social networking sites.

Please note: Sunnyside Nursery does not recommend the use of photographs and video featuring children on sites such as Facebook and (X formally Twitter), due to issues with obtaining parental consent and the inability to ensure that the privacy of those children can be safeguarded on social networking sites.

Mobile/Smart Phones

Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and smart phones are familiar to children outside of nursery. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in nursery is allowed. Sunnyside chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices

- Sunnyside Nursery allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does Sunnyside Nursery allow a member of staff use this device whilst working and/or whilst in environments where children are present.
- Users who bring personal devices into nursery must ensure there is no inappropriate or illegal content on the device.
- Sunnyside Nursery is not responsible for the loss, damage or theft of any personal mobile device.

School Provided Mobile Devices

- Where Sunnyside Nursery provides mobile technologies such as phones, laptops and PDAs for offsite visits and trips, only these devices should be used.

- Where Sunnyside Nursery provides a laptop for staff, only this device may be used to conduct nursery business outside of nursery.

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.

As photographs and video of children and staff are regarded as personal data in terms of the Data Protection Act (1998) we must have written permission for their use from the individual or their parent/carer. At Sunnyside we are aware of the issues surrounding the use of digital media online. All members of our nursery understand these issues and must follow the nursery's guidance. We seek written consent from parents/carers and staff who appear in the media. Parental/carer permission is obtained annually. Parents/carers are made aware that we retain images after children have stopped attending Sunnyside Nursery. Parents/carers and staff are aware that full names and personal details will not be used in any digital media, particularly in association with photographs.

Generally, the use of videos and cameras is not permitted, unless operated by an authorised member of staff, with nursery equipment and for nursery purposes. When taking photographs/video, staff ensures that children are appropriately dressed and are participating in activities that develop learning.

Storage of Images

- Images/films of children are stored on the nursery's network.
- Staff are not permitted to use portable media storage of images (e.g. USB sticks) without express permission of the nursery manager.
- Rights of access to this material are restricted to the teaching staff within the confines of the nursery network.

Webcams and CCTV

Sunnyside Nursery uses CCTV for security and safety. The only people with access to this area are the Manager and Deputy. Webcams are (occasionally) used by staff for meetings with Sunnyside Nursery.

Laptops/iPads/Tablets

Staff Use:

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

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

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

• Nursery 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 and this must be acknowledged during all stages of employment.

Children's Use:

• Laptop, iPad 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 by the Manager.

• 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 nursery device.

Applications (Apps) for recording pupil progress

In recent years, a number of applications (apps) for mobile devices have been launched which are targeted specifically at Early Years Practitioners and settings. Many of these apps allow staff to track and share a child's learning journey online with parents and carers, usually in the form of photographs and text. Such tools have considerable benefits, including improved levels of engagement with parents and a reduction in paperwork, but careful consideration must be given to safeguarding and data security principles before using such tools.

- Personal staff mobile phones or devices (e.g. iPad or iPhone) should not be used for any apps which record and store children's personal details, attainment or photographs. Only nursery issued devices may be used for such activities, ensuring that any devices used are appropriately encrypted if taken off site. This is to prevent a data security breach in the event of loss or theft.

Data Storage and Security

In line with the requirements of the Data Protection Act (1988), sensitive or personal data is recorded, processed, transferred and made available for access in nursery. This data must be accurate; secure; fairly and lawfully processed, for limited purposes and in accordance with the data subjects rights; adequate, relevant and not excessive; kept no longer than necessary; and only transferred to others with adequate protection.

At Sunnyside Nursery we specify how we keep data secure and inform staff as to what they can/cannot do with regard to data through this eSafety policy. Tara Lougheed is responsible for managing information. ICT enables efficient and effective access to and storage of data for the management team, staff and administrative staff. Sunnyside Nursery complies with LEA requirements for the management of information in nursery. Only trained and designated members of staff have authority and access rights to input or alter data.

Sunnyside has defined roles and responsibilities to ensure data is well maintained, secure and that appropriate access is properly managed with appropriate training provided. Our files and network system are backed up weekly so that copies of the data will always be available. Backup is managed by the manager; this is done at the end of the week. Approved anti-virus software is updated regularly on all IT (ipads/smartboard/laptops etc) by the manager.

- All laptops and computers are password protected. All work email accounts are password protected. A secure email facility is available for staffs that need to send confidential information.
- Passwords should contain at least eight characters and contain upper and lower case letters as well as numbers. Passwords should be easy to remember, but hard to guess. Staff should not share their passwords with anyone; write their passwords down or save passwords in web browsers if offered to do so.
- Staff should not use their username as a password. Staff should not email their password or share it in an instant message. Staff should change their password if they think someone may have found out what it is.
- Staff should be aware of who they are allowed to share information with. Clarification can be obtained from the manager. Sensitive information should only be sent via the secure email system.
- Don't assume that third-party organisations know how your information should be protected. The use of unencrypted memory storage devices to store information of a personal sensitive or confidential nature is not permitted.

- Staff should only download files or programs from trusted sources. If in doubt, advice should be sought from the Manager.
- Staff should lock sensitive information away when left unattended.
- Unauthorised people should not be allowed into staff areas.
- Computer screens should be positioned so that they cannot be read by others who shouldn't have access to that information. Confidential documents should not be left out.
- Staff should only take information offsite when authorised and only when necessary. On occasions when this is necessary, staff should ensure that the information is protected offsite in the ways referred to above. Staff should be aware of their location and take appropriate action to reduce the risk of theft.
- Staff should ensure that they sign out completely from any services they have used, for example email accounts. Staff should try to reduce the risk of people looking at what they are working with. Laptops should not be taken abroad (some countries restrict or prohibit encryption technologies).

What is On-Line Abuse

Online abuse is any type of abuse that happens online. It can happen via any device that is connected to the Internet i.e. computers, iPads, tablets, and mobile phones. It can also happen anywhere online, including:

- social media
- text messages and messaging apps
- emails
- online gaming
- live-streaming sites
- online chat rooms

Dealing with e-safety incidents

Sunnyside Nursery endeavours to prevent any e-Safety incidents occurring and ensure that children's use of our devises is safe and that children and staff information is protected at all times. However, in the event of an e-Saftey incident of concern involving a child and/or staff occur a full investigation and/or safeguarding (child protection) procedures will be enforced (see safeguarding policy). Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the nursery Manager Tara and/or Shalina (Deputy). Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported. All e-safety incidents should be recorded in an 'e-safety Incident Log'. See **Appendix A** for an example:

Incident Reporting

Appendix A

E Safety Incident Log					
Date of Incident	**Name of individual(s) involved**	**Device number/location**	**Details of incident**	**Actions & reasons**	**Confirmed by**
01/01/2021	Joe Bloggs	Ipad rm.2 ground floor	Child accessed inappropriate content	Practitioner informed Manager, incident log filled out and IT provider called. Suspended use of all devises. Websites blocked and filtering levels reviewed and altered. Safeguarding flow chart consulted.	Manager & Deputy

Details of ALL eSafety incidents will be recorded by staff and monitored monthly by the Provider/Manager.

Useful links

- Data Protection and Freedom of Information advice: www. ico.org.uk
- The UK Safer Internet Centre, has information on e-safety tips, advice and resources to help children and young people stay safe on the internet.
  Contact Details:
  The helpline 0344 381 4772 is open from 10 am to 4pm.
  Email: helpline@saferinternet.org.uk
  Website: http://www.saferinternet.org.uk/

E-Safety Policy

This policy is checked annually and formally reviewed at least every 3 years and/or revised as required by legislation, government guidance and/or feedback from service users.

This policy supports all other policies and must be read together with the following policies:

- Acceptable Use Policy'
- Safeguarding
- GDPR

This policy was adapted in December 2023 and due for review in December 2024
