E Safety Policy for Early Years Settings

Ronald Tree Nursery

This policy was last reviewed on 18th April 2018

Karen Sharman, Head Teacher

Policy Statement

The internet is an accessible tool to children in early years settings- gaming, mobile learning apps etc

All early years settings 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, however it is likely that we will never be able to completely eliminate them. 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 offer valuable guidance and resources to early years settings and practitioners 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.
- 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, 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 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.

Staff 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 attached Acceptable Use Policy for Early Years Employees 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, students or committees.

Network Manager/Technical Staff (if applicable)

(Please note: If using an outside contractor for technical services, it is the responsibility of the setting to ensure that the managed service provider carries out all of the safety measures listed below that would be expected of in-house technical staff, including being provided with the Early Years e Safety Policy and Staff AUP)

The Network Manager/Systems Manager/ICT Technician 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 and that responsibility for its implementation is shared with the E Safety Lead and the Designated Person for Safeguarding.
- any problems or faults relating to filtering are reported to Designated Person for Safeguarding and to the broadband provider immediately and recorded on the e Safety Incident Log.
- users may only access the setting's network through a rigorously enforced password protection policy, in which passwords are regularly changed.
- he/she keeps up to date with e safety technical information in order to maintain the security of the network and safeguard children.
- the use of the setting's network is regularly monitored in order that any deliberate or accidental misuse can be reported to the E Safety Lead/Designated Person for Safeguarding.

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 regardless of the size of the setting.

Before investing in a broadband connection, it is important that early years settings carefully consider their internet requirements and usage. **Domestic lines may not be appropriate to the needs of an early years setting**, particularly with regards to the security of any data within the network and the requirement to provide appropriate filtering for young users. It is ultimately the responsibility of the Provider/Manager to ensure that the setting's internet provision is as safe and secure as is reasonably possible.

Possible statements:

Larger settings

- Filtering levels are managed and monitored on site via an administration tool/control panel, provided by our broadband supplier, which allows an authorised staff member to instantly allow or block access to sites and manage user internet access.
- Filtering levels are managed and monitored on behalf of the setting by our broadband supplier or technical support, allowing an authorised staff member to allow or block access to site 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 internet access in line with user requirements (e.g. Youtube at staff level but blocked to children)
- Any changes to filtering levels are documented on the Filter Change Request Log *(see attached template document)* and include the reason for the requested change, the date and name of staff member concerned.

Smaller settings

- Parental controls are established on all internet enabled devices that children have access to, blocking or preventing access to any harmful, illegal or inappropriate content.

Indicators of inadequate or poor practice

- There is no filtering or monitoring in place
- Security of passwords is ineffective (e.g. passwords are shared amongst staff and pupils or children log-in using staff accounts)
- All users (i.e. staff and children) access the same level of filtering resulting in either staff being restricted as to what they can view, or children accessing too much.

Email Use

Staff

- The setting provides keyworker 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.
- 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. This prohibits contact with former pupils outside of authorised setting email channels also.
- All emails should be professional in tone and checked carefully before sending, just as an official letter would be.

Use of Social Networking Sites (advertising or parental contact)

Social networking sites (e.g. Facebook and Twitter) can be a useful advertising tool for early years settings and can often be an effective way of engaging with young 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.
- 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 refer to the attached Social Networking Policy for further guidance.

Please note: LSCBN does not endorse the use of photographs and video featuring children and young people on sites such as Facebook and Twitter, due to issues with obtaining parental consent and the inability to ensure that the privacy of those young people can be safeguarded on social networking sites.

Mobile/Smart Phones

Staff:

- Personal mobile phones are permitted on setting grounds, but are to be used during break times only, within designated areas away from children.
- 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. Setting 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 in the policy.

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.

- Written consent must be 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. However, in exceptional circumstances, such as equipment shortages, permission may be granted by the Provider/Manager for use of personal equipment for setting related photographs or videos, provided that the there is an agreed timescale for transfer and deletion of the image from the staff member's device.
- Setting 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 in the policy. In the case of an outing, all data must be transferred/deleted from the setting's camera/device before leaving the setting.

Laptops/iPads/Tablets

Staff Use:

- A log of all ICT equipment issued to staff, including serial numbers, is maintained by the Network Manager or ICT Co-ordinator.
  Personal use of setting laptops or computing facilities, whilst on site, is left to the discretion of the Provider/Manager and may be permissible if kept to a minimum, used outside of session times. Please refer to the attached AUP and Social Networking Policy for further guidance.
- Where staff have been issued with a device (e.g. setting laptop) for work purposes, personal use whilst off site is not permitted unless authorised by the provider/manager. 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 setting laptops and devices are made available as necessary for anti-virus updates, software installations, patches, upgrades or routine monitoring/servicing.
- Setting 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 in the policy.
- Please note: The Provider/Manager is ultimately responsible for the security of any data or images held of children within the setting.

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 by the Provider/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 setting 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 setting 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**.
- Before purchasing or accessing any apps for staff or children's use, Providers/Managers must have a clear understanding of where and how children's data will be stored, including who has access to it and any safeguarding implications. Please note: The Provider/Manager is ultimately responsible for the security of any data or images held of children within the setting.

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.

Useful links

- Local Safeguarding Children Board Northamptonshire (LSCBN). Online Procedures: www.lscbnorthamptonshire.org.uk

- Northamptonshire County Council E safety pages: www.northamptonshire.gov.uk/en/councilservices/EducationandLearning/services/ict/Pages/e-safety.aspx

- Data Protection and Freedom of Information advice: www. ico.org.uk

Incident Reporting

Filtering Change Log

All filtering change requests to be recorded by Network Manager or staff member authorised to adjust filtering levels. All filtering changes must be authorised by Provider/Manager.

Website / category	Date	Requested by / reason	Authorised by	Change made by	Confirmed by	Date for review

E Safety Incident Log

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

Date of incident	Name of individual(s) involved	Device number/location	Details of incident	Actions and reasons	Confirmed by