E-Safety Policy

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

- For the management team to offer valuable guidance and resources to parents 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, 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.

At Grass Roots Private Day Nursery we provide a diverse, balanced and relevant approach to the use of technology. Children are encouraged to maximise the benefits and opportunities that technology has to offer. Children learn in an environment where security measures are balanced appropriately with the need to learn effectively. Our nursery community understands the importance of an e-Safety Policy.

Staff Responsibilities

Management Team

The role of the management team includes:

- Ensuring that the e-Safety 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 e-Safety incident occur
- Ensuring that the e-Safety incident log is appropriately maintained and reviewed regularly;
- Ensuring e-Safety updates, training and advice is available for staff, parents/carers and volunteers;
- Liaison with Senior Designated Person(s) to ensure a coordinated approach across relevant safeguarding issues.

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.

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 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.

Email Use for Staff

- The setting has 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 practice 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, threatening or bullying in nature.

Use of Social Networking Sites (advertising or parental contact)

Social networking sites (e.g. Facebook, Instagram 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 note: Grass Roots Private Day Nursery does not endorse the use of photographs and video featuring children and young people on sites such as Facebook, Instagram 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/ Watches

Grass Roots Private Day Nursery chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices **see also Mobile Phone Policy*

- Grass Roots Private Day Nursery allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the nursery allow a member of staff to use this device whilst working.

- Practitioners are not able to have access to their mobile phones or any other electronic device that accepts calls, messages and video calling whilst they are working to ensure that they are completely attentive to the needs of the children.
- A smart watch may be worn if the above functions are switched off during work time.
- Users bringing personal devices into nursery must ensure there is no inappropriate or illegal content on the device.
- The nursery is not responsible for the loss, damage or theft of any personal mobile device.

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 pupils 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. We ensure that any photographs or recordings taken of the children in our setting are only done with prior written permission from each child's parent. This is gained when each child starts with us. We ask for individual permissions for photographs and video recordings for each different use including, use in the child's learning journey, for display purposes, for promotion materials including our nursery brochure and to use in the local press. We ensure that parents/carer(s) understand that their child may also be on another photograph, but not as the primary person, that may be used in another child's learning journey. If a parent is not happy about one or more of these uses then the nursery will respect their wishes and find alternative ways of recording their child's play or learning.
Staff are not permitted to take photographs or recordings of a child on their own cameras, mobiles or other devices and only use those provided by the nursery.

In our nursery we are aware of the issues surrounding the use of digital media online. All members of our nursery understand these issues and need to 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 using the setting. 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. The use of videos and cameras is not permitted in the setting, unless by an authorised member of staff with nursery equipment and for nursery purposes. When taking photographs/video, staff ensures that subjects are appropriately dressed and are not participating in activities that could be misinterpreted.

The nursery management team will monitor all photographs and recordings to ensure that the parent's wishes are adhered to. Parent/carer(s) are not permitted to use any recording device or camera (including those on mobile phones) on the nursery premises without the prior consent of the management team. During special events, e.g. Christmas or leaving parties, permission is gained from each parent before the event and a briefing is given to all parent/carer(s) before any photos are taken about their acceptable use in relation to social media.
If any parent/carer(s) are unhappy about photos being taken then a member of staff may produce a group photograph to distribute to parent/carer(s) on request, this will ensure all photographs taken are in line with parental choice.
The nursery has computers which will be used for the storage of photographs of the children in our care. Each computer has a password to protect from misuse and therefore can only be accessed by nursery staff. When a child leaves the setting any photos are removed from that computer by the management team.

Storage of Images

- Images/films of children are stored on the nursery's cloud storage and downloaded to the network as needed.

- Staff are not permitted to use portable media storage of images (e.g. USB sticks)
- Rights of access to this material are restricted to the staff within the confines of the nurseries network

Computers/iPads/Tablets

Staff Use:

- Where staff have been issued with a device (e.g. setting tablet) for work purposes, personal use whilst on or off site is not permitted unless authorised by the management team. The settings 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 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.

Children's Use:

- Tablet/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 management team.
- 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.
- The nursery ensures that any programmes watched are suitable for all the children in their care.

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 will be given to safeguarding and data security principles before using such tools.

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; 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.

Our online cloud storage systems are password protected and can only be accessed via permission from the management team.

At Grass Roots Private Day Nursery we specify how we keep data secure and inform staff as to what they can/cannot do with regard to data through this e-Safety policy.

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 off site 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.

Serious Incidents

If a serious incident occurs such as inappropriate content is accessed, an e-safety incident log should be made immediately, the manager is informed and the use of nursery computers is suspended until the management team has dealt with the issue.

Useful links

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

This policy will be reviewed by management annually, who are responsible for ensuring the dissemination of this policy to all staff, volunteers and parents.

E-Safety Incident Log

Date of Incident	Name of individuals involved	Device Location	Details of Incident	Actions and Reasons	Confirmed by