

E-Safety Policy

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.

•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.

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 Daisy Chains 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 school community understand the importance of an eSafety Policy.

Practitioners

Our eSafety Champion is Ashley Scholfield.

The role of the eSafety Champion in our setting includes:

•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.

•Ensuring eSafety updates, training and advice is available for staff and parents/carers.

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

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/tablet 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.

Photographs and Videos

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. In our nursery we are aware of the issues surrounding the use of digital media online. All members of our team understand these issues and need to follow the Daisy Chains policies and procedures.

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 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.

The use of videos and cameras is not permitted in the nursery, unless by an authorised member of staff with nursery equipment and for nursery purposes.

Storage of Images

•Images/films of children are stored on the nursery computers.

•Staff are not permitted to use portable media storage of images (e.g.

USB sticks) without permission off a manager.

•Rights of access to this material are restricted to the staff within the nursery.

Webcams and CCTV

Daisy Chains uses CCTV for security and safety. The only people with access to this area are the management team.

Laptops/i-pads/tablets

Staff Use:

•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, 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 authorised by management team.

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 management.

•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 Online Learning Journeys

 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.

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 school. This data must be accurate; secure; fairly and lawfully process; 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 Daisy Chains 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. Ashley Scholfield is responsible for managing information. ICT enables efficient and effective access to and storage of data for the management team and staff.

Daisy Chains has defined roles and responsibilities to ensure data is well maintained, secure and that appropriate access is properly managed with appropriate training provided.

All laptops and computers are password protected. All work email accounts are password protected.

Staff should be aware of who they are allowed to share information with. Clarification can be obtained from the management team. 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.

Staff should only download files or programs from trusted sources. If in doubt, advice should be sought from management team.

Staff should lock sensitive information away when left unattended. Unauthorised people should not be allowed into the office or staff room. 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.

Serious incident

If a serious incident occurs such as inappropriate content is accessed, the e safety incident log is made immediately, the nominated officer is informed and the use of classroom computers is suspended until the computer has been checked and ensured that the pathway is blocked.

Useful Links

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

|  |  |  |  |
| --- | --- | --- | --- |
| **This policy was reviewed on** | **Nursery Staff Signature** | **Date disseminated to staff** | **Date for review** |
| January 19 |  |  | January 20 |