E-Safety Policy for Early Years Settings

Appletree Nursery School

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.

At Appletree 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.

Staff Responsibilities
Practitioners (including volunteers)

Our eSafety Champion is Christine Branscombe

The role of the eSafety Champion in our school 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 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) to ensure a coordinated approach across relevant safeguarding issues.

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 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.

- Filtering levels are managed and monitored on behalf of the setting by our technical support (Prescotts)

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.

- 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 is 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 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.

.

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 school. 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 school is allowed. Appletree choses to manage the use of these devices in the following ways so that users exploit them appropriately.

Personal Mobile Devices

- Appletree allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does Appletree allow a member of staff use this device whilst working.

- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

- Appletree is not responsible for the loss, damage or theft of any personal mobile device.

School Provided Mobile Devices

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

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

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. In our school we are aware of the issues surrounding the use of digital media online. All members of our school understand these issues and need to follow the school'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 Centre. 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 Centre, unless by an authorised member of staff with school equipment and for school purposes.

When taking photographs/video, staffs ensures that subjects are appropriately dressed and are not participating in activities that could be misinterpreted.

Storage of Images

- Images/films of children are stored on the school's network.

- Staff are not permitted to use portable media storage of images (e.g. USB sticks) without express permission of the head teacher.

- Rights of access to this material are restricted to the teaching staff within the confines of the school network

Webcams and CCTV

Webcams are used by staff for meetings with Stoneygate Nursery School

Laptops/iPads/Tablets

Staff Use:
- 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 headteacher. The settings laptop/devices should be used 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.

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 headteacher.
- 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.**

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 Appletree 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. Julie Morrow is responsible for managing information. ICT enables efficient and effective access to and storage of data for the management team, staff and administrative staff.

The centre complies with LEA requirements for the management of information in centres. We currently use SIMS administrative network and this is supported by the BTlancashire . Only trained and designated members of staff have authority and access rights to input or alter data.

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

The computer network within the school has security against access to the management system. The files and network system are backed up daily so that copies of the data will always be available. Backup is managed on line by Mozy,

this is done every evening. Tec Hub also check that the backup is working properly.

Approved anti-virus software is updated regularly on all IT (ipads/smartboard/laptops etc) by Tec Hub. 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 Head. 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.

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).

Serious Incidents

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

Useful links

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

Incident Reporting

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
1/10/12	Joe Bloggs	PC 63 Rm 4	Child accessed inappropriate content	Teacher informed nominated officer, incident log filled out and IT provider called. Suspended use of computers in classroom. Website now blocked and filtering levels reviewed and altered.	Davey Jones (Deputy Head CPO)