E-Safety Policy

Statement of Intent

At Bybrook Pre-school, we recognise the value that communication and technology plays in the learning and development of the children. Children are given regular access to ICT equipment, to develop skills that are vital to life-long learning.

We acknowledge that there are potential risks involved, and therefore follow this policy to ensure E-Safety is followed for the benefit of the children, parents, staff and visitors to the pre-school.

It is our intention to provide an environment in which children, parents and staff are safe from images being recorded and inappropriately used in turn eliminating the following concerns: 1) Staff being distracted from their work with children; 2) The inappropriate use of mobile phone cameras around children.

Procedures

1. ***Information Communication Technology (ICT) equipment***
    - Only ICT equipment belonging to the setting is used by staff and children.
    - The designated person is responsible for ensuring all ICT equipment is safe and fit for purpose.
    - All computers have virus protection installed.
    - The designated person ensures that safety settings are set to ensure that inappropriate material cannot be accessed.

2. ***Internet Use***
    - Children do not normally have access to the internet and never have unsupervised access.
    - If staff access the internet with children for the purposes of promoting their learning, written permission is gained from parents who are shown this policy.
    - The designated person has overall responsibility for ensuring that children and young people are safeguarded and risk assessments in relation to online safety are completed.
    - Children are taught the following stay safe principles in an age appropriate way prior to using the internet;
        - only go on line with a grown up
        - be kind on line
        - keep information about me safely
        - only press buttons on the internet to things I understand
        - tell a grown up if something makes me unhappy on the internet
    - Designated persons will also seek to build children's resilience in relation to issues they may face in the online world, and will address issues such as staying safe, having appropriate friendships,

asking for help if unsure, not keeping secrets as part of social and emotional development in age appropriate ways.

- If a second hand computer is purchased or donated to the setting, the designated person will ensure that no inappropriate material is stored on it before children use it.
- All computers for use by children are located in an area clearly visible to staff.
- Children are not allowed to access social networking sites.
- Staff report any suspicious or offensive material, including material which may incite racism, bullying or discrimination to the Internet Watch Foundation at www.iwf.org.uk
- Suspicions that an adult is attempting to make inappropriate contact with a child on-line is reported to the National Crime Agency's Child Exploitation and Online Protection Centre at www.ceop.police.uk**.**
- The designated person ensures staff have access to age-appropriate resources to enable them to assist children to use the internet safely.
- If staff become aware that a child is the victim of cyber-bullying, they discuss this with their parents and refer them to sources of help, such as the NSPCC on 0808 800 5000 or www.nspcc.org.uk, or Childline on 0800 1111 or www.childline.org.uk
- Staff using personal computers at home for the purposes of work are made aware that they should be protected by secure passwords and have recognised spyware software installed.

3. Emails

- The pre-school has a designated email address for professional correspondence that is password protected. The password is only known by the Pre-school Leader and Chair of the Pre-school Management Committee. It is changed at regular intervals, and if the Pre-school Leader or Chair leave. If the password is divulged, this is a breach of confidentiality and is treated as such.
- Children are not permitted to use email in the setting. Parents and staff are not normally permitted to use setting equipment to access personal emails.
- Staff do not access personal or work email whilst supervising children.
- Staff send personal information by encrypted email and share information securely at all times.

4. Personal Emails

It is recognised that the Pre-school Leader, Staff and Pre-school Management Committee may communicate via email outside of working hours. The pre-school advises that all personal computers are locked with a security password and have spyware software installed.

All emails should adhere to the following:

- The names of children should be kept to a minimum
- Correspondence should be polite, respectful and remain professional
- Any abuse or breaches of confidentiality by any adults/students associated with the pre-school is strictly forbidden, and will not be tolerated.
- All suspected cases must be reported, the pre-school will record all incidents and act on them immediately.

5. Storage of Documentation

Bybrook Pre-school recognises that personal computers are used to create working documents such as registers, invoicing and planning.

- Access to documents with personal information is limited as much as possible, and is usually only available to the Pre-school Leader, Chair of the Pre-school Committee and Treasurer
- All home computers must be password protected
- Work documents placed in locked folders
- Only acceptable use is permitted
- Personal details are kept to a minimum
- All confidentiality is assured, with breaches considered serious misconduct, and dealt with accordingly

6. Social Media

Bybrook Pre-school has a Facebook page and Twitter account. The pages do not feature any children's photos, or use the name of any child. Any abuse or breaches of confidentiality by any adults/students associated with the pre-school is strictly forbidden, and will not be tolerated. All suspected cases must be reported, the pre-school will record all incidents and act on them immediately.

- Confidentiality by staff is ensured within their terms and conditions of employment, any reported breach of confidence is considered gross misconduct and will result in instant dismissal.
- Staff, parents or committee members should not upload photos taken of children in setting to any social network site. Parents are reminded of this at occasions where photographs are taken (sports day, nativity etc)
- Students on commencement of placement sign to say they will abide by our student policy and maintain confidentiality at all times. Any reported breach of this agreement will result in immediate termination of their placement with the pre-school, and notification to their educational establishment.

7. Use of Cameras

- Personal cameras belonging to staff are not permitted in the pre-school.
- The pre-school provides an authorised digital camera for use by staff. Under no circumstances should photos be taken on a mobile phone.
- Parental permission is sought before any photographs are taken of children
- All staff are made aware of any parental photographic objections or restrictions.
- Staff are permitted to take children's photographs to capture spontaneous moments to support the Early Years Foundation Stage or to share with parents, once consent is granted.
- Images taken must be deemed suitable without putting the child/children in any position that could cause embarrassment or distress.
- All staff are responsible for the location of the camera; this should be placed within the lockable cupboard when not in use.
- The camera must be locked away at the end of every session.
- Images taken and stored on the camera must be downloaded and then erased as soon as possible (and within a week)

- Photographs should then be distributed to members of staff (key persons) to record in children's learning journals.
- Under no circumstances must cameras of any kind be taken into the bathrooms without prior consultation with the Pre-school Leader.
- If photographs need to be taken in a bathroom, i.e. photographs of the children washing their hands, then the Pre-school Leader must be asked first and staff be supervised whilst carrying out this kind of activity. At all times the camera must be placed in a prominent place where it can be seen.
- If photographs of children are used for publicity purposes, parental consent must be given and safeguarding risks minimised, for example, ensuring children cannot be identified by name or through being photographed in a sweatshirt with the name of their setting on it.
- Failure to adhere to the above will lead to disciplinary procedures being followed.
- Parents are permitted to take photos during organised events such as Sports Day and the Nativity. Parents are reminded that photos should be for personal use only, and not uploaded to any social networking site or webpage.

8. Mobile Phones

- Children do not bring mobile phones or other ICT devices with them to the setting. If a child is found to have a mobile phone or ICT device with them, this is removed and stored in the kitchen until the parent collects them at the end of the session.
- The pre-school has an authorised mobile phone for use in setting, as there is no landline available in the hall. All contact details for children are kept in the filling cabinet and no numbers are stored in the pre-school mobile.
- Staff mobile phones are kept in the kitchen and should not be used during pre-school hours. Under no circumstances does the pre-school allow a member of staff to contact a parent/carer using their personal phone.
- Staff must ensure that their mobile phones which are bought into setting, do not have any inappropriate or illegal content on. Under no circumstances should a member of staff use their phone to take photos in setting.
- Staff needing to use a phone in setting (due to personal reasons/ an emergency) etc, do so at the discretion of the Pre-school Leader, Designated Safeguarding Lead or Chair or the Pre-school Committee. If a member of staff has a family emergency or similar and it is necessary to keep their phone to hand, prior permission should be sought from the Pre-school Leader and the mobile phone can be placed by the kitchen hatch. Any personal phone calls should be taken in the committee room.
- During outings and walks, the Pre-school takes responsibility for the phone and a contact list, to ensure parents can be contacted in case of an emergency.
- Parents and visitors are requested not to use their mobiles within the pre-school and are asked to sign the Visitors policy to acknowledge this.
- If a visitor needs to use their mobile phone in order to fulfil the reason for their visit/job, then they will ask permission from the Pre-school Leader or Designated Safeguarding Lead and be supervised at all times.

- It is the responsibility of all members of staff to be vigilant and report any concerns to the Pre-school Leader. Concerns will be taken seriously, logged and investigated appropriately (under the Allegations against Staff policy).
- The Pre-school Leader reserves the right to check the image contents of a member of staff's mobile phone should there be any cause for concern over the appropriate use of it.
- Should inappropriate material be found then our Local Authority Designated Officer (LADO) will be contacted immediately. We will follow the guidance of the LADO as to the appropriate measures for the staff member's disciplinary action.

Further guidance

- NSPCC and CEOP *Keeping Children Safe Online* training: www.nspcc.org.uk/what-you-can-do/get-expert-training/keeping-children-safe-online-course/

Responsibilities

The responsibilities of the Pre-School Leader are:

- to ensure that all members of staff have read and understood this policy, and to make them aware of the severity of their actions should they choose not to put the policy into practice.
- to make sure the parents are aware of this policy.

The responsibilities of employees are:

- to read and confirm understanding of this policy.
- to work according to the terms set out in this policy.

The responsibilities of parents are:

- to be aware of this policy and what measures can be taken at home to keep children safe from harm regarding e-safety.

The responsibilities of the members of the Pre-school Management Committee are:

- to ensure that all members of staff have read and understood this policy, and to make them aware of the severity of their actions should they choose not to put the policy into practice.

This policy was adopted at a meeting of Bybrook Pre-school Management Committee held on:
16th January 2016

Date of review: 16th January 2017

Signed on behalf of the Pre-school Management Committee:

Name of signatory: Role of signatory:

Signed on behalf of the pre-school:

Name of signatory: Role of signatory:

Guidelines for pre-school staff using Social Networking Sites

Social networks are very popular and used by all ages in society. The most popular social networks are web-based, commercial, and not designed for educational use. They include sites like Facebook and Twitter. For individuals, social networking sites provide tremendous potential opportunities for staying in touch with friends and family.

As childcare workers we have a professional image to uphold and how we conduct ourselves online helps determine this image. As reported by the media, there have been instances of childcare professionals demonstrating professional misconduct while engaging in inappropriate dialogue about their setting and/or children, staff and parents; or posting pictures and videos of themselves engaged in inappropriate activity. Increasingly, staffs' online identities are too often public and can cause serious repercussions, both privately and professionally.

One of the hallmarks of social networks is the ability to "friend" others – creating a group of others that share interests and personal news. You are advised not to accept invitations to *friend* parents or carers within these social networking sites. When children and parents gain access into a worker's network of friends and acquaintances and are able to view personal photos, the dynamic is altered. 'Friending' children and parents provide more information than one should share in an educational setting. It is important to maintain a professional relationship to avoid relationships that could misconstrued; and/or are contrary to the 'Guidance for Safer Working Practices for Adults who Work with Children and Young People (November 2007).

For the protection of your professional reputation, it is expected that you comply with the following practices:

Friends and friending

- Do not accept parents and carers as friends on personal social networking sites.
- Do not initiate friendships with parents
- Remember that people classified as "friends" have the ability to download and share your information with others.

Content

- Do not write or respond to anything deemed to be defamatory, obscene, proprietary, or libellous. Exercise caution with regards to exaggeration, colourful language, guesswork, obscenity, copyrighted materials, legal conclusions, and derogatory remarks or characterisations.
- Weigh whether a particular posting puts your effectiveness as a childcare professional at risk.
- Post only what you want the world to see. Imagine that all work contacts are able to visit the site. It is not like posting something to your web site or blog and then realizing that a story or photo should be taken down. On a social networking site, basically once you post something it may be available, even after it is removed from the site.
- Do not discuss children, parents or co-workers or publicly criticize the pre-school's policies, activities or personnel.
- Do not post images that include childcare and/or parents.

Security

- Visit your profile's security and privacy settings. At a minimum, childcare professionals should have all privacy settings set to "only friends".
- "Friends of friends" and "Networks and Friends" open your content to a large group of unknown people. Your privacy and that of your family may be a risk. People you do not know may be looking at you, your work, your home, your kids, your grandchildren - your lives!