Little Swans Day Nursery *e – Safety Policy*

Reviewed by: Elaine Boulton nursery owner
Date of Review: June 2017

This e-Safety Policy is used in conjunction with other nursery policies; Behaviour, Anti-bullying and Child Protection

New technologies have become integral to the lives of our children both within our setting and in their lives outside.
This e-Safety Policy explains how the nursery intends to do this, whilst also addressing wider education issues in order to help staff parents and carers to be responsible users whilst using the internet and other communications technologies for educational, personal and recreational use.

- Little Swans Day Nursery has appointed **Mrs Samantha Tranter, Nursery Manager** to be the *E – Safety* Co-ordinator.

Miss Tranter will have the overall legal, personal and moral responsibility to ensure online safety will be effectively considered. She will not only be responsible for the safety of our children and young people within the nursery, but also for the behaviours and expectations of any adults who affect or come into contact with the nursery. This list should not be considered exhaustive.

1. Background and Purpose

1.1 New technologies have become integral to the lives of children and young people in today's society, both within nursery and in their lives outside of nursery

1.2 The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students/children learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children should have an entitlement to safe internet access at all times.

1.3 The requirement to ensure that children are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in nurseries are bound. The nursery e-Safety policy should help to ensure safe and appropriate use. The development and implementation of such a strategy should involve all of the stakeholders in a child's education from senior management, to the senior leaders, support staff members of the community and the children themselves.

1.4 The use of these exciting and innovative tools in nursery and at home has been shown to raise educational standards and promote child achievement.
However, the use of these new technologies can put children at risk within and outside of the setting. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing personal information
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/ contact with others, including strangers
- Access to unsuitable video/ internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excess use which may impact on the social and emotional development and learning of the child

1.5 Many of these risks reflect situations in the off-line world and it is essential that this e-Safety policy is used in conjunction with other nursery policies (e.g. Behaviour, Anti-bullying and Child Protection).

1.6 As with all other risks, it is impossible to eliminate those risks completely: it is therefore essential, through good educational provision to build staff and children's resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

1.7 The nursery must demonstrate that it has provided the necessary safeguards to help ensure that they have done everything that could reasonably be expected of us to manage and reduce these risks. The e-Safety policy that follows explains how we intend to do this, whilst also addressing wider educational issues in order to help staff, children and their parents and carers to be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

2. Scope

2.1 This policy applies to all members of Little Swans Community (including staff, students/children, volunteers, parents, carers, visitors and community users who have access to and are users of the nursery ICT systems, both in and out of nursery.

2.2 The Education and Inspections Act 2006 empowers management to such extent as is reasonable, to regulate the behaviour of staff and children when they are off the nursery premises and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-Safety incidents covered by this policy, which may take place outside of nursery, but is linked to membership of Little Swans.

2.3 The nursery will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents and appropriate adults of inappropriate e-Safety behaviour that takes place outside of the setting.

3. Roles and Responsibilities

3.1 The following sections outline the roles and responsibilities for e-Safety:

3.2 Management and Senior Leaders

- Management is responsible for ensuring the safety (including e-safety) of members of the community, though the day to day responsibility for e-safety will be delegated to the e-safety co-ordinator, Sam Tranter
- The owner is responsible for ensuring that the e-safety coordinator and other relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant
- The management /senior leaders will ensure that there is a system in place to allow for monitoring and support of those in nursery who carry out the internal e-safety monitoring role. This is to provide a safety net and also support those colleagues who take on important monitoring roles
- The Senior Management Team will receive regular monitoring reports from the e-safety coordinator/officer
- Management and another member of the Senior Management Team/ should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff

3.3 E-safety coordinator

> leads on e-safety
> Takes a day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the nursery e-safety policies/documents
> Ensures that all staff is aware of the procedures that need to be followed in the event of an e-safety incident taking place
> provides training and advice for staff
> liaises with nursery ICT technical staff
> receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments

The officer is also responsible for ensuring:

- That the nurseries ICT infrastructure is secure and is not open to misuse or malicious attack
- That the users may only access the nurseries networks through a properly reinforced password protection policy
- That the nurseries filtering policy is applied and updated on a regular basis
- That she keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
- That monitoring software / systems are implemented and updated as agreed in nursery policies

3.4 **Teaching and support staff**

Are responsible for ensuring that:

- They have an up to date awareness of e-safety matters and of the current nursery e-safety policy and practices

- They have read and understood and signed the nursery Staff Acceptable Use Policy
- They report any suspected misuse or problem to the appropriate person for investigation
- Digital communications with staff should be on a professional level and only carried out using official nursery communication systems
- E-safety issues are embedded in all aspects of the curriculum and other nursery activities

Designated senior person for child protection should be aware of:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate on-line contact with adults/strangers

3.5 Education and Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly. It is expected that some staff will identify e-safety as a training need within the performance management process
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the nursery e-safety policy and Acceptable Use Policy
- There will be regular reviews and audits of the safety and security of nursery ICT systems

3.6 Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The nursery will therefore take every opportunity to help parents understand these issues through parent's evenings, newsletters, website as well as local e-safety campaigns/literature. Parents and carers will be responsible for:

- Accessing the nursery website/children's records in accordance with the relevant nursery Acceptable Use Policy

- Children's on-line Learning Journey and daily reports system is hosted on secure dedicated servers based in the UK. Access to information `Your Learning Journals` can only be gained by name, unique id and password. Parents can only see their own child's information and are unable to login to view other children's Learning Journeys.

4. Policy Statements

Staff should act as good role models in their use of ICT, the internet and mobile devices

- There is a yearly review of the safety and security of nursery ICT systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to nursery ICT systems
- The administrator passwords for the nursery ICT system, used by management must also be available to other nominated senior leaders
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- The nursery has provided appropriate user-level filtering through the use of the filtering programme

- In the event of management (or other person) needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by management (or other nominated senior leader).
- Requests from staff for sites to be added or removed from the filtered list will be actioned by management
- Nursery management can monitor and record the activity of users on the nursery ICT systems and users are made aware of this in the Acceptable Use Policy
- An agreement is in place for the provision of temporary access of "guests" onto the nursery system. Both computers in the main office have guests accounts
- A written agreement is in place regarding the use of removable media (e.g. memory sticks / CDs / DVDs) by users on nursery workstations/portable device
- The nursery infrastructure and individual workstation that are connected to the internet are protected by up to date virus software
- Personal data cannot be sent over the internet or taken off the nursery site unless safely encrypted or otherwise secure

4.1 Use of Images

- Staff is allowed to take and use images to support educational aims, but must follow nursery policies concerning the sharing, distribution and publication of those images. Those images should only be taken on nursery equipment; the personal equipment of staff should not be used for such purposes
- Care should be taken when taking images that children are not participating in activities that put them at risk or bring the individuals or the nursery into disrepute
- Photographs published on the website, or elsewhere that include children will be selected carefully and will comply with good practiced guidance on the use of such images
- Children's full names will not be used anywhere on a website or blog, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs of children are published on the nursery website
- Children's work can only be published with the permission of the children's parent or carer

5. The Use of Email

5.1 Electronic mail (e-mail) is now an important means of communication for most members of nursery. Messages can be delivered almost anywhere in the world rapidly and it is simple to generate, reply to, or forward an e-mail

5.2 There are responsibilities involved in using e-mail. In signing the Nursery Acceptable Use Policy all employees agree to fulfil these responsibilities and acknowledge the wider MoD Policy and UK Data Protection law

5.3 General considerations when using E-mail

- E-mail is not a confidential means of communication. Staff should bear in mind that e-mail messages can be very easily read by those for whom they were not intended and in particular recognise that e-mails can be:

- Intercepted by a third party
- Wrongly addressed
- Forwarded accidently
- Forwarded by initial recipients to third parties against your wishes
- Viewed accidently on recipient's computer screens
- Sensitive personal data should not be communicated by e-mail unless the express permission of the subject has been obtained or unless adequate encryption facilities have been employed.
- Staff must not include any defamatory comments in any e-mail messages. E-mail is a form of publication and the laws relating to defamation apply. A comment made in jest can be misinterpreted by its recipient. In- for example- a case of harassment it is the effect of as communication which is considered and not the intention of the sender
- Staff must never use a false identity in e-mails, and must be aware that there is no guarantee that the e-mail received was in fact sent by the purported sender. If, for any reason, an e-mail is sent on behalf of someone else the sender must make that clear at the beginning of the message
- The nursery e-mail system must not be used to create or distribute unsolicited offensive or unwanted e-mail, including the dissemination of chain letters. The sending of unsolicited marketing messages is now a criminal offence
- E-mails that show the nursery in an unprofessional light or that could expose nursery to illegal liability must not be sent by any member of staff. E-mails sent by a member of staff have the same standing as a letter on headed note paper even if the contents are described as "private". As such all communications are subject to the Data Protection Act
- Be very careful when downloading material from the internet and opening external e-mails if there is any suspicion of it including a virus. If you have any suspicions, do not open an attachment and contact the nursery management immediately
- Staff must not invade anyone's privacy by any means using e-mail
- E-mail is not a substitute for record keeping purposes. Where long term accessibility is an issue staff must transfer e-mail records to a more lasting medium or another electronic environment
- The laws applying to copyright apply to email messages and attachments. Staff must familiarise themselves with nursery policies in relation to copyright and be careful when copying material for inclusion in e-mail
- Documents attached to e-mails may contain information from which the history of a documents creation may be deducted. This data may identify those involved in generating or altering that item
- Personal data is subject to the Act. Under its terms, personal data includes any information about a living identifiable individual, including his/her name, address, phone number, and e-mail address. If you include such information in an email or an attachment to an email, you are deemed to be "processing" personal data and must abide by the Act. Personal information includes any expression of opinion
- Putting personal information (and especially personal sensitive information) in an unencrypted email bears significant risk and is not an acceptable practice. The use of a "safe haven" fax machine or suitably double-enveloped letter must be considered for the sending of all such information
- Staff must not collect such information without the individual knowing what it is to be used for and how it might be transmitted to third parties. Information so collected must not be disclosed or amended except in accordance with the purpose for which the information was collected. Information must be accurate and up to date
- Nursery has by law to provide any personal information held about any data subject who requests it under the Act. This includes information on individual PCs in areas where the Pc is connected to the internet and all staff has a responsibility to comply with any instruction to release such data made by

nursery Data Protection Lead. Emails which contain personal information and are held in live, archive or back-up systems or have been "deleted" from the live systems, but are still capable of recovery, may be accessible by data subjects.

- The law also imposes rules on the retention of personal data. Such data should be kept only for as long as it is needed for the purpose for which it was collected.
- Care must be taken when sending e-mails containing personal information to countries outside the European Economic Area, especially if those countries do not have equivalent levels of protection for personal data

6. Social Networking

6.1 Acceptable **use of Social Networking Sites**

6.2 The widespread availability and use of social networking applications bring opportunities to understand engage and communicate with our audiences in new ways. It is important that we are able to use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with our duties to our services users and partners, our legal responsibilities and our reputation
6.3 for example, our use of social networking applications has implications for our duty to safeguard children and young people
6.4 The requirements set out below aim to provide this balance to support innovation whilst providing a framework of good practice
Social networking applications include, but are not limited to:

- Blogs
- Online discussion forums
- Collaborative spaces
- Media sharing services e.g. YouTube
- Micro logging
- applications e.g. Twitter

6.5 many of the principles of this policy also apply to other types of online presence such as virtual worlds and the use of any such service must be discussed with Miss Tranter, nursery manager before use

6.6 Uses in Nursery

6.7 The use of social networking sites within the setting is only allowed in appropriately controlled situations and in support of legitimate curriculum activities – for example to teach the safe use of the internet
*** Staff** and students must not access the social networking sites for personal use via nursery information systems, nursery networks or using nursery equipment
* If staff access social networking sites using their personal computer systems and equipment, they should never give out personal information of any kind which could identify themselves, colleagues and or pupils
* staff must not place inappropriate photographs on any social network space and must – where they do post photographs – ensure that background detail e.g. house number, street name etc. cannot identify them. Photographs of colleagues and or children – taken for example on school trips – must not be posted without the express permission of parents for those in the photographs or their parents/carers
* Staff is strongly advised not to communicate with students over social network sites using their personal systems and equipment

* Staff must not run social network spaces for work experience students use on a personal basis. If social networking is used for supporting students with coursework professional spaces must be created by staff for use by students

6.8 Nurseries are vulnerable to material posted about them online and all staff should be made aware of the need to report this should they become aware of anything bringing the nursery into disrepute. Nurseries are advised to check regularly, using a search engine, to see if any such material has been posted.

6.9 If staff use social networking sites they should not publish specific and detailed "personal views" relating to the nursery staff or students.

6.10 The nursery network and IT facilities must not be used for the following activities:

* conducting illegal activities
* accessing or downloading pornographic material
* gambling
* Soliciting for personal gain or profit
* Managing or providing a business or service
* Revealing or publicising proprietary or confidential information
* Representing personal opinions
* making or posting indecent or offensive remarks or proposals

6.11 Terms of Use

6.12 All proposals for using social networking applications as part of Nursery (Whether they are hosted by the nursery or a third party) must be approved by Samantha Tranter

6.13 All staff must adhere to these terms of use. The terms of use below apply to all users of social networking applications by all staff. This includes, but is not limited to, public facing applications such as open discussion forums and internally-facing uses such as project blogs regardless of whether they are hosted on corporate networks or not

6.14 Nursery expects that users of social networking applications will always exercise the right of freedom of expression with due consideration for the rights of others and strictly in accordance with these Terms of use

6.11 Legislation

6.12 The following legislation – enforceable against public sector employees including nursery staff – must be considered when using the internet or email:

- Human Rights Act 1998
- Regulation of Investigatory Powers Act 2000 (RIPA) 3
- Data Protection Act 1998
- Freedom of information Act 2000
- Copyrights, Designs and Patents Act 1988, amended by the Copyright and Related Rights Regulations 2003
- Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Obscene Publications Act 1959, Protection of Children Act 1988, Criminal Justice Act 1988

6.13 These Acts are concerned with material that might be

- Criminal
- Cause harm to young people or
- Be otherwise unlawful

6.14 Enforcement

6.15 Any breach of the terms set out below can result in the application or offending content being removed in accordance with the published complaints procedure and the publishing rights of the responsible nursery employee being suspended

6.16 The nursery reserves the right to require the closure of any applications or removal of content published by nursery representatives which may adversely affect the reputation of nursery or put it at risk of legal action

6.17 Any communications or content you publish that causes damage to the nursery, any of its employees or any third-party reputation may amount to misconduct or gross misconduct to which the nursery Dismissal and Disciplinary Policies apply

7 Data Protection

7.1 The Data Protection Act (DPA) applies to all establishments wherever located.
Staff must thus ensure that they:

- Keep personal data in a secure environment, minimising the risk of its loss or misuse
- Use personal data only on the nursery computers in the office which are password-protected, ensuring they are properly “logged –off” at the end of any working session.
- Transfer data using encryption and secure password protected devices.

7.2 When using communication technologies nursery must consider the following as good practice:

- Users need to be aware that email communications are not secure and can be monitored
- Users must immediately report, to Miss Tranter or Mrs Boulton the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email
- Any digital communication between staff /parents or carers may be subject to data protection requests and must be professional in tone and content

8. Misuse

8.1 Misuse of nursery electronic and telecommunications equipment is a serious disciplinary Offence

8.2 Nursery management can exercise a right to monitor the use of nurseries information systems and internet access. This includes the right to intercept email and delete inappropriate materials where unauthorised use of the nursery’s information system may be taking place, or the system may be used for criminal purposes, or for storing unauthorised text, imaginary or sound.

8.3 Staff must be aware that improper or unacceptable use of the internet, email and equipment could result in legal proceedings and the use of the nursery’s disciplinary procedure.

8.4 Sanctions will depend on the gravity of misuse and could result in dismissal
8.5 All employees should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and freedom of information legislation, the Safeguarding Vulnerable Groups Act 2006 and other relevant legislation. They must also operate in line with the nursery's equality and diversity policies and procedures.

8.6 Misuse by staff

8.7 If a member of staff is believed to misuse the internet in an abusive or illegal manner, a report must be made to the nursery management immediately and then the nursery Allegations against Staff procedure and the Child Protection Policy must be followed to deal with any misconduct and all appropriate authorities will be contacted.
8.8 Allegations are defined as information relating to either potential criminal conduct or a conduct raising concerns about a person's suitability.

Other Useful Information and Contacts:

SWGfl Staying Safe
http://www.swgfl.org.uk/Staying-Safe
Collection of advice, support and resources for early Years practitioners and their managers, children and young people, parents and carers

Childnet International
http://www.childnet-int.org/
Wide range of resources, in particular the acclaimed "Know IT All for Parents and Carers".

The Byron Review
http://www.dcsf.gov.uk/byronreview/

Click Clever Click Safe
The first UK Child Internet Safety Strategy (UKCCIS UK Council for Child Internet Safety).

A Parent's guide for Online Safety for Under Fives

You should start talking to your child about keeping safe online at an early age. It's easier to have conversations about online safety little and often, rather than trying to cover everything at once.

- Set boundaries from the start. It makes it easier than trying to play catch –up at a later stage.
- Check that websites are suitable before your child visits them. Look for websites that have parental pages that explain how the site works and how they keep your child safe.
- Ensure your home page is set to a child-friendly website.
- Talk to friends about what websites their children use.
- Play games with your child to get them used to being online.
- Set 'Safety Mode' up on YouTube to help filter out explicit content.
- If you use Google, turn on Google **'safe search'** to filter sexually explicit content from your search results.

Form more help and advice visit

www.nspcc.org.uk/onlinesafety

Or contact the NSPCC helpline on 0808 800 5000 to discuss any concerns