Selly Oak Nursery School
26 Tiverton Road, Selly Oak, Birmingham B29 6BP
Tel: 0121 472 1700 Fax: 0121 472 7252
Email: enquiry@sellyoak-nur.bham.sch.uk
Website: www.sellyoak-nur.bham.sch.uk

SELLY OAK NURSERY SCHOOL

E-SAFETY POLICY FOR SCHOOL

RIGHTS RESPECTING SCHOOL

This policy is in accordance with the 1989 United Nations Convention on the Rights of the Child (UNCRC)
Article 17 Every child has the right to reliable information from the media. This should be information that children can understand. Governments must help protect children from materials that could harm them.
Article 28 Every child has the right to an education.

1. Introduction

1.1 The governing body of Selly Oak Nursery School has adopted this policy to help the school meet its responsibilities for safeguarding and educating children, for regulating the conduct of employees and for complying with legislation covering the use of information and communication technologies and digital and mobile devices.

1.2 This policy was adopted by the governing body on Selly Oak Nursery School and will be reviewed annually in the light of guidance from the local authority or earlier if the local authority issues further guidance in the light of particular circumstances or developments in information and communication technology.

2. Basic principles

2.1 In adopting this policy the governing body has taken into account the expectation by Ofsted that rigorous e-safety policies and procedures are in place in the school, written in plain English, with contributions from the whole school, updated regularly and ratified by governors.

2.2 The policy applies to all members of the school community, including staff, pupils, volunteers, parents and carers, governors, visitors and community users who have access to, and are users of, the school's information and communication technology systems or who use their personal devices in relation to their work at the school.

2.3 The governing body expects the head teacher to ensure that this policy is implemented, that training in e-safety is given high priority across the school, that consultations on the details of the arrangements for e-safety continue with all employees on a regular basis, and that any necessary amendments to this policy are submitted to this governing body for approval.

2.4 The principal context for this policy is the need to safeguard children. It will be applied in conjunction with the procedure for safeguarding children approved by the Birmingham Safeguarding Children Board. It will also be applied in conjunction with the school's behaviour and anti-bullying policies for pupils and with the rules and procedures governing the conduct of employees.

2.5 The governing body expects the head teacher to arrange for this policy to be published to all employees and volunteers in the school and for necessary instructions and guidance, particularly on acceptable use, to be given to pupils in a manner suited to their ages and abilities.

3. Roles and responsibilities

Governing body

3.1 The governing body will consider and ratify this e-safety policy, and review it annually in the light of guidance from the local authority, or sooner if the local authority issues new guidance in the light of

particular circumstances or developments in information and communication technology. Governors are expected to follow the policy in the same way as volunteers are expected to follow it, including participating in e-safety training if they use information and communication technology in their capacity as school governors.

3.2 Governors are responsible for ensuring that proper procurement procedures are used if they decide to purchase information technology services from an external contractor and that City Council or other reputable specialist advice is taken on the specification for those services to ensure proper security and safeguarding of children.

Head teacher

3.3 The head teacher is responsible for ensuring that:

- the governing body is offered appropriate support to enable this policy and its application to be reviewed regularly, and to ensure that other school policies, including that on pupils' behaviour, take account of this e-safety policy;
- the governing body is given necessary advice on securing appropriate information and communication technology systems;
- the school obtains and follows City Council or other reputable guidance on information and communication technology to support this policy;
- take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the e-safety policy
- the school has senior teachers to co-ordinate e-safety.
- there is effective consultation with all employees, and other users of the school's information and communication technology systems, to take account of the particular features of those systems and educational, technical and administrative needs;
- the school provides all employees with training in e-safety relevant to their roles and responsibilities
- that training is also provided to volunteers and school governors who use information and communication technology in their capacity as volunteers or governors, as the case may be;
- pupils are taught e-safety as an essential part of the curriculum;
- the senior leadership team is aware of the procedures to be followed in the event of a serious e-safety incident, including an allegation made against an employee, and that all employees know to whom they should report suspected misuse or a problem ;
- records are kept of all e-safety incidents and that these are reported to the senior leadership team;
- necessary steps have been taken to protect the technical infrastructure and meet technical requirements of the school's information and communication technology systems;
- there is appropriate supervision of, and support for, technical staff;
- any outside contractor which manages information technology for the school undertakes all the safety measures which would otherwise be the responsibility of the school to the standard required by the school and is fully aware of this policy and that any deficiencies are reported to the body which commissioned the contract.
- provide and coordinate e-safety advice / guidance / training as required to individuals and groups in the community

Other employees

3.4 Other employees are responsible for:

- undertaking such responsibilities as have been delegated by the head teacher commensurate with their salary grade and job descriptions;
- participating in training in e-safety provided by the school and in consultations about this policy and about its application, including e-safety within the curriculum;
- using information and communication technology in accordance with this policy and the training provided;
- reporting any suspected misuse or problem to the person designated by the school for this purpose.
- having read, understood and signed the Safeguarding policy

- being aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current policies with regard to these devices

Pupils

3.5 Pupils are expected to use information and communication technology systems and devices as they have been taught and in accordance with the school's behaviour policy and the instructions given to them by staff.

Other users

3.6 Volunteers, including governors, who help in the school and who use information and communication technology systems and devices in helping the school are expected to

- participate in training in e-safety provided by the school and in consultations about this policy and about its application, including e-safety within the curriculum;
- use information and communication technology in accordance with this policy and the training provided;
- report any suspected misuse or problem to the person designated by the school for this purpose.

Parents

3.7 Parents who help in the school as volunteers are covered by 3.6 above. Parents who are not voluntary helpers in the school are nonetheless subject to the law in the event of misuse of information and communication technology.

4. Acceptable use

4.1 The use of information and communication technology should follow the following general principles:

- This policy should apply whether systems are being used on or off the school premises.
- The school's information and communication technology systems are intended primarily for educational use and the management and administration of the school. During work breaks appropriate, reasonable personal use is permitted.
- Data Protection legislation must be followed.
- Users must not try to use systems for any illegal purposes or materials.
- Users should communicate with others in a professional manner.
- Users must not disclose their password and they should not write it down or store it where it is possible that another person might steal it. Users must not attempt to use another person's user-name or password.
- Users must report as soon as possible any apparently illegal, inappropriate or harmful material or event to the person designated by the school.

4.2 Employees, volunteers and governors should:

- not open, copy, remove or alter any other user's files without that person's express permission;
- only take and/or publish images of other people with their permission, or, in the case of pupils, the permission of their parents or guardians;
- when recording or publishing such images for educational purposes should not attach to those images any names or other personal information enabling identification;
- as far as possible communicate with pupils and parents only through the school's official communication systems and not publish personal contact details through those systems;
- if they occupy a senior post in which they need to keep e-mail and other messages confidential, ask the school for a separate e-mail address for this purpose;
- if they use personal devices during their work (subject to the agreement of the school in the case of employees), ensure that the systems which they use are secure, protected with passwords and encrypted;
- not use personal social networking sites through the school's information and communication technology systems;
- not open any hyperlinks in, or attachments to, e-mails, unless the source is known and trusted;
- ensure that their data is backed-up regularly in accordance with the rules of the school's systems;
- only download or upload large quantities of information if they have permission to do so, in order to avoid overloading the school's systems;

- not try to install any programmes or alter any computer settings unless this is allowed under the rules for the school's information and communication technology systems;
- not deliberately disable or damage any information and communication technology equipment;
- report any damage or faults to the appropriate member of staff.

5. Social Media

Use of social media networks or sites, whether by pupils or employees, should be subject to the same standards as the school would expect for behaviour and conduct generally (as set out in the school's code of conduct for support staff and the Teachers' Standards for teachers). The school accepts the separation of private life and work and will not concern itself with people's private lives unless it appears that the law has been broken, or that an employee is in breach of contract, or that the school is, or will be, brought into disrepute.

5.1 **Personal Use by staff**

The personal use of social media can lead to unintended consequences and when innocent actions are misconstrued or misinterpreted. Caution is advised when inviting work colleagues to be 'friends' in personal social networking sites.

Staff members are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. Staff members should keep their passwords confidential, change them often and be careful about what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information. It is a good idea to use a separate email address just for social networking so that any other contact details are not given away.

In order to avoid these issues and protect themselves on social media, staff must ensure that:

- they do not identify themselves as employees of Selly Oak Nursery School in their personal webspace. This is to safeguard the privacy of staff members, particularly those involved in providing sensitive frontline services
- they do not have contact through any personal social medium with any parents
- they do not use any information gained as part of their role at Selly Oak Nursery for personal gain or pass this information onto others who may use it in such a way
- they do not contact parents via social media websites after leaving their employment at Selly Oak Nursery School
- they do not discuss or reveal any information they have access to as part of their employment, including personal information about children and their family members, colleagues, Local Authority staff and other parties
- they do not publish photographs, videos or any other types of image of children and their families or images depicting staff members wearing Selly Oak Nursery School clothing on their personal webspace
- Selly Oak NurserySchool email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media

Using Social media on behalf of Selly Oak Nursery School

5.2 Social media can be a powerful communications tool and allow Selly Oak Nursery School to forge stronger links with parents and families. To ensure the safeguarding of children and to help project the school's ethos of caring professionalism, staff must:

- not disclose information, make commitments or engage in activities on behalf of Selly Oak Nursery School without authorisation
- provide worthwhile and accurate information; remember what is published on the site will reflect Selly Oak Nursery School's image, reputation and services.
- stay within the law and be aware that child protection, privacy, data protection, libel, defamation, harassment and copyright law may apply to the content of social media
- respect their audience and be sensitive in the tone of language used and when discussing topics that others may find controversial or objectionable

- seek permission from the relevant people before citing or referencing their work or referencing service providers, partners or other agencies
- never give out their personal information such as home contact details or home email addresses on social media
- not express personal opinions on official sites and social media representing the school.

Careful consideration must be given to the level of engagement of contributors – for example whether users will be able to add their own text or comments or upload images. Only staff members who have been trained on the use of social media will be given permission by SLT to manage the school's website or social media accounts.

Behaviour likely to cause extreme offence, for example racist or homophobic insults, or likely to put a young person or adult at risk of harm must never be tolerated. Such comments must never be posted or removed immediately and appropriate authorities, for example the Police or Child Exploitation and Online Protection Centre (CEOP), informed in the case of illegal content or behaviour.
Parents/carers must never post images which contain other children on social media sites.

6. Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning. However, staff and children need to be aware of the risks associated with sharing images and with posting digital images on the internet.

- Staff will take digital/video images to support educational aims, but must follow policies concerning the sharing, distribution and publication of those images
- Care should be taken when taking digital / video images that children are appropriately dressed
- Photographs published on the website or elsewhere that include children will be selected carefully and will comply with good practice guidance on the use of such images.
- Children's full names will not be used anywhere on a website, blog or social media, particularly in association with photographs
- Written permission from parents or carers will be obtained before photographs and videos of children are published on the school website or on school social media

7. Education and training

7.1 Education and training in e-safety will be given high priority across the school.

7.2 The education of pupils in e-safety is an essential part of the school's e-safety provision and will be included in all parts of the curriculum.

7.3 The school will offer education and information to parents, carers and community users of the school about e-safety.

7.4 Suitable training will be provided through the school for all employees, as part of induction and subsequently during their employment in the school. There will be a regular review of the training needs of all staff and the content of training should be kept up to date. The training will be linked to training about child protection and data protection. It will cover related matters such as the law on copyright of electronic materials.

7.5 Volunteers and governors who use information and communication technology during their work will be offered the same training as employees.

8. Data Protection

8.1 The school will ensure that its information and communication technology systems are used in compliance with current data protection legislation and that all users are made aware of the school's data protection policy, including the requirement for secure storage of information.

9. Technical aspects of e-safety

9.1 The school will seek to ensure that the information and communication technology systems which it uses are as safe and secure as is reasonably possible by taking reputable advice and guidance on the technical requirements for those systems.

9.2 The school will undertake regular reviews of the safety and security of its information and communication technology systems.

9.3 Particular attention will be paid to secure password protection and encryption for devices located in the school and mobile devices.

9.4 The school's systems will also provide for filtering internet access for all users, preventing access to illegal content, and with additional filtering for different groups of users for inappropriate content.

9.5 The school will ensure that its information and communication technology systems include standard, automated monitoring for illegal materials, profanity, and unsolicited materials (generally known as 'spam'). It should safeguard children and adults against inappropriate use. It should provide the head teacher and senior leadership team with regular reports to indicate whether or not there have been any incidents.

9.6 Additional monitoring may take place as part of an investigation following evidence of apparent misuse.

10. **Dealing with incidents**

10.1 Any suspicions of misuse or inappropriate activity related to child protection should be reported as prescribed in the Safeguarding Board's child protection procedures.

10.2 Any suspicions of other illegal activity should be reported to the head teacher, who should take advice from appropriate persons (according to the nature of the suspected activity and the individuals apparently involved) and, depending on the advice and the outcome of preliminary investigations, should report alleged criminal activity to the police and may also instigate disciplinary procedures.

10.3 Suspicions of inappropriate, as distinct from illegal, use of information and communication technology should be reported to the head teacher or other designated member of the senior leadership team for investigation and appropriate action. This may lead to informal management discussions, improved training or, depending on the nature of the alleged misuse, investigation under the disciplinary procedure for employees, or the school's behaviour policy for pupils.

Agreed by Selly Oak Nursery School Governing Body:-

Signed ……

Date.....

Review……

APPENDIX Information for Parents

Latest Ofcom research has shown that 91% of 5-15 year olds live in a household with internet access and over a third of all 3-4 year olds are now accessing the internet in their homes. We know that children need support in these environments, to get the best out of using the internet, and there are real advantages in making sure that children are supported in their internet use right from the start.

Children can be enthusiastic users of technology. The challenge can be to harness this enthusiasm and ensure a balance, so that the use of technology does not negatively impact on other important areas of young children's lives.

Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyberbullying
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the child.

There are some strategies that can be used to help manage the time online issue, such as agreeing time limits or using time limiting tools, designating weekly times to use the internet together.

Where to start?

The best way to keep your family safe online, and to understand your children's internet use, is to use the internet together. Active engagement and conversations with your children are key. Be positive and embrace the technologies that young children enjoy and look for family activities or games. Take time to explore the games and services that your children are using, or want to use, and look out for any safety features that may be available. This will give you a better understanding of the different ways that children are engaging with technology and help you to feel more confident.

Should I set any rules?

In the same way that you set rules for most areas of your children's lives, establish your expectations regarding online activities. Creating a family agreement is a useful step, which might include time spent online, sites that can be visited, and behaviour expected; remember, what's right and wrong offline is also right and wrong online. It's a great idea to agree these rules from the outset, so that you and your children are aware of their boundaries.

How can I supervise my child?

Placing your computer or laptop in a busy part of the house e.g. the living room or kitchen can be helpful. This can make it easier for you to be involved in their technology use. But remember, the internet can be accessed from a number of portable devices, for example smartphones, iPod Touch, games consoles and tablets. Portable devices may allow you to ensure your children are using them where you can see them and your children can still be supervised.

Tools to help

There are free parental controls and filters available, to help you set safer boundaries for your children, but you will usually be required to set them up. Your internet service provider will provide free filters to help block age inappropriate content for children, and on the UK Safer Internet Centre website you can watch video tutorials that show you how to find and set these up. All mobile phone operators also provide such parental controls for free. The websites of device manufacturers (such as games consoles) should also outline the controls to which you have access.

Filtering options can be found within websites and services themselves, for example on YouTube or 'safe search' settings can be applied to search engines such as Google or Bing. There are even some search services designed for children (such as Yahoo! Kids). Parental controls can be password protected, so it's advisable to choose a strong password and not share it. Parental controls and filters are a good starting point but it is important to recognise that they are not 100% effective. They are a great help, but not a solution, and work best in combination with parental supervision and engagement, to help your children understand how to stay

safe online. As children grow and develop, so do their online needs, therefore you may want to periodically review your parental controls to accommodate this.

Top Tips!

- **Talk to your child about what they're up to online**. Be a part of their online life; involve the whole family and show an interest. Find out what sites they visit and what they love about them, if they know you understand they are more likely to come to you if they have any problems.
- **Encourage your child to go online and explore!** There is a wealth of age-appropriate sites online for your children. Encourage them to use sites which are fun, educational and that will help them to develop online skills.
- **Keep up-to-date with your child's development online**. Children grow up fast and they will be growing in confidence and learning new skills daily. It's important that as your child learns more, so do you.
- **Set boundaries in the online world just as you would in the real world**. Think about what they might see, what they share, who they talk to and how long they spend online. It is important to discuss boundaries at a young age to develop the tools and skills children need to enjoy their time online.
- **Keep all equipment that connects to the internet in a family space**. For children of this age, it is important to keep internet use in family areas so you can see the sites your child is using and be there for them if they stumble across something they don't want to see.
- **Know what connects to the internet and how**. Nowadays even the TV connects to the internet. Make sure you're aware of which devices that your child uses connect to the internet, such as their phone or games console. Also, find out how they are accessing the internet – is it your connection, or a neighbour's wifi? This will affect whether the safety setting you set are being applied.
- **Use parental controls on devices that link to the internet, such as the TV, laptops, computers, games consoles and mobile phones**. Parental controls are not just about locking and blocking, they are a tool to help you set appropriate boundaries as your child grows and develops. They are not the answer to your child's online safety, but they are a good start and they are not as difficult to install as you might think. Service providers are working hard to make them simple, effective and user friendly.

Top Tips! Encourage your child to:

- **Always ask a grown up** before you use the internet. They can help you find the best thing to do.
- **Don't tell strangers** where you live, your phone number or where you go to school. Only your friends and family need to know that.
- **Don't send pictures** to people you don't know. You don't want strangers looking at photos of you, your friends or your family.
- **Tell a grown up** if you feel scared or unhappy about anything.

Useful websites

www.thinkuknow.co.uk/parents

www.saferinternet.org.uk

www.protectingourchildren.co.uk/
www.bbc.co.uk/cbbc/topics/stay-safe
www.kidsmart.org.uk