E-SAFETY POLICY
September 2023

Introduction

New technologies have become integral to the lives of children and young people in today's society and the increased provision of the internet inside and outside of school brings with it the need to ensure that learners are safe.

At LPEBL we provide pupils with minimal exposure to screens. Pupils in Year 5 and 6 will on occasion be given computer access at school with adult supervision for certain projects linked to the curriculum. They will occasionally be given certain projects to do at home that may involve internet research and use of powerpoint presentations.

We have a duty to teach pupils how to evaluate internet information and to take care of their own safety and security. E-safety, which encompasses internet technologies and electronic communications, will educate pupils about the benefits and risks of using technology and provide safeguards and awareness to enable them to control their online experience.

Aims

- This is a whole school policy to ensure all members of the school community make use of the internet and other technologies for appropriate professional and educational purposes.
- To ensure that Internet use and use of related technologies is monitored and managed appropriately.
- To provide a mechanism by which staff and pupils are protected from sites, information and individuals that could undermine the principles and aims of the school.
- To promote responsible behaviour with regard to online activities and foster the critical thinking skills necessary to enable pupils to remain safe online.

The proprietor has:

- appointed the Headteacher to be the Coordinator for E-Safety.
- delegated powers and responsibilities to the Head Teacher to ensure all school personnel and visitors to the school are aware of and comply with this policy.

The Headteacher will:

- ensure all school personnel, pupils and parents are aware of and comply with this policy.
- work with the Governing Body to create a safe ICT learning environment by:
    - having in place a comprehensive policy for pupils, staff and parents.
    - ensure that all Internet users are kept up to date with new guidance and procedures.

- have editorial responsibility for the school website and will ensure that content is accurate and appropriate.
- monitor the implementation of this policy and its effectiveness
- ensure all Anti-Virus software is updated on all devices.

- undertake training in order to understand e-safety issues and procedures.
- ensure that the School has an effective filtering policy in place and that it is applied and updated on a regular basis.

School Staff will:

- comply with all the aforementioned aspects of this policy.
- accept the terms of and sign the staff "Acceptable Use Staff Agreement Form"
- be responsible for promoting and supporting safe behaviours with pupils and e-safety procedures.
- undertake appropriate training.
- ensure mobiles are only used in designated areas (staffroom or offices).
- All staff are aware that technology can play a significant part in many safeguarding and wellbeing issues and that pupils are at risk of abuse online as well as face-to face. Staff are also aware that, sometimes, such abuse will take place concurrently online and during a pupil's daily life.
- Staff are expected to be alert to the possibility of pupils abusing their peers online and to understand that this can occur both inside and outside of school.
- It is important that staff recognise the indicators and signs of child on child abuse, including where such abuse takes place online, and that they know how to identify it and respond to reports. Staff must also understand that, even if there are no reports of child on child abuse at the School, whether online or otherwise, it does not mean that it is not happening; it may simply be the case that it is not being reported.
- It is important that staff challenge inappropriate behaviours between peers and do not downplay certain behaviours, including sexual violence and sexual harassment, as "just banter", "just having a laugh", "part of growing up" or "boys being boys" as doing so can result in a culture of unacceptable behaviours, an unsafe environment for children and, in a worst case scenario, a culture that normalises abuse. The School has a zero tolerance approach towards child on child abuse (including in relation to sexual violence and sexual harassment) and such behaviour is never acceptable and will not be tolerated. The School will treat any such incidences as a breach of discipline and will deal with them under the School's Behaviour Policy and also as a safeguarding matter under the School's Safeguarding and Child Protection Policy and procedures.
- Staff have a responsibility to report any concerns about a pupil's welfare and safety in accordance with this policy and the School's Safeguarding and Child Protection Policy. If staff have any concerns regarding child on child abuse or if they are unsure as to how to proceed in relation to a particular incident, they should always speak to the Designated Safeguarding Lead in all cases.

- Training of all staff includes online safety which, amongst other things, includes an understanding of filtering and monitoring provisions in place, how to manage them effectively, how to escalate concerns when identified and any particular expectations or responsibilities in relation to filtering and monitoring.

Pupils in older classes will be taught to:

- **be critically aware of the materials they read.**
- **validate information before accepting its accuracy.**
- **acknowledge the source of information used.**
- **use the Internet for research.**
- **respect copyright when using Internet material in their own work.**

Parents/carers will:

- be aware of and comply with this policy.
- make their children aware of the e-safety policy.
- when in school, turn off mobiles or have them on silent.

Where accessible to the pupils, the school Internet will:

- be designed for pupil use with adult supervision.
- be reviewed and improved at regular intervals.

Authorisation of Internet Access:

- Before using any school ICT resource, all staff must read and sign the 'Acceptable Use Staff Agreement Form'
- All up to date records will be kept of all pupils and school personnel who have Internet access.

The School Website

Contact details on the website will be:

- the school address,
- e-mail address and
- telephone number.

The school website will not publish:

- staff or pupils contact details;
- the pictures of children without the written consent of the parent/carer;
- the names of any pupils who are shown;
- children's work without the permission of the pupil or the parent/carer.

Social Networking

Pupils will not be allowed access to social networking sites.

Netiquette

Netiquette is a term referring to good behaviour while connected to the Internet. Netiquette is mainly referring to behaviour while using Internet facilities such as individual websites, emails, newsgroups, message boards, chat rooms or web communities. The following rules, for staff and pupils, will ensure that we are well-mannered when communicating electronically:

- **Do not use someone else's name and pretend to be them.**
- **Do not try to obtain someone else's password.**
- **Do not call anyone names or threaten them with personal violence.**
- **Never forget that the person reading your mail is, indeed, a person, with feelings that can be hurt.**
- **Do not send anonymous messages.**
- **Write clearly and succinctly.**
- **Do not forward chain letters or unsolicited e-mails.**
- **Do not attach large files unless absolutely necessary.**
- **Do not use capital letters in messages (this is considered to be shouting).**
- **Proof read before you send.**
- **Check your emails regularly.**
- **Acknowledge that you have received a document.**

Adult Code of Conduct for Safe Use of Technology

Mobile phone use:

- **Only use your phone during school breaks.**
- **Switch off your phone and store in your bag.**
- **Never phone parents or school agencies from your own phone.**
- **Never take photos of children with your phone without permission from the headteacher.**
- **Never give your phone number to children or parents.**
- **Never send text messages about children or their parents on your phone.**

Computer safety:

- **Never tell children your personal email address.**
- **Never communicate with children on social networking sites.**
- **Never send photos of children on the internet.**
- **Always send confidential information (i.e. with children's names) securely, in a manner consistent with agreed school policy.**
- **Never keep photos or films of children on your phone or USB stick.**
- **Do not keep confidential information on a USB stick.**
- **Do not allow children in your care to have unsupervised access to computers.**

Camera use:

- **Never take a school camera or the school ipad home.**
- **Do not allow non staff access to our photos without express permission from the parents, in writing and with the permission of the HeadTeacher.**

- **Do not allow non staff to photograph our children without written permission from parents given through the Head Teacher.**

How complaints regarding E-Safety will be handled

The school will take all reasonable precautions to ensure e-safety. However, owing to the size and nature of the internet, the availability of mobile technologies and the speed at which technologies change, it is not possible to guarantee that unsuitable material will never appear on a school website. The school cannot accept liability for material accessed in school, nor any consequences of Internet access. The Head Teacher acts as the first point of contact for any complaint. The Head Teacher will deal with all complaints of Internet misuse by school personnel.

Complaints of cyberbullying are dealt with in accordance with our Behaviour Policy. Complaints related to child protection are dealt with in accordance with stated school procedures.

Education in E-Safety

La Petite Ecole Bilingue will work to raise the awareness and importance of safe and responsible use of the internet and related technologies. The children will be taught rules that will help to protect them when using the Internet. Children will be supported in making informed and appropriate choices if they encounter people and material online that may be challenging, prejudiced, inaccurate or that promote an extreme lifestyle or point of view.

Pupils are educated in an age appropriate manner about the importance of safe and responsible use of technology, including the internet, social media and mobile electronic devices.

Technology is included in the educational programmes followed in the EYFS in the following ways:

- children are guided to make sense of their physical world and their community through opportunities to explore, observe and find out about people, places, technology and the environment;
- children are enabled to explore and play with a wide range of media and materials and provided with opportunities and encouragement for sharing their thoughts, ideas and feelings through a variety of activities in art, music, movement, dance, role-play, and design and technology; and
- children are guided to recognise that a range of technology is used in places such as homes and schools and encouraged to select and use technology for particular purposes.

The safe use of technology is also a focus in all areas of the curriculum teacher training and key safety messages are reinforced as part of assemblies, PSHE and tutorial / pastoral activities, teaching pupils:

- about the risks associated with using the technology and how to protect themselves and their peers from potential risks;

- about the importance of identifying, addressing and reporting inappropriate behaviour, whether on or offline, and the risks of downplaying such behaviour as, for example, "banter" or "just boys being boys";
- to be critically aware of content they access online and guided to validate accuracy of information;
- how to recognise suspicious, bullying or extremist behaviour;
- the definition of cyberbullying, its effects on the victim and how to treat each other's online identities with respect;
- relevant laws applicable to the internet
- the consequences of negative online behaviour;
- how to report cyberbullying and / or incidents that make pupils feel uncomfortable or under threat and how the School will deal with those who behave badly; and
- how to respond to harmful online challenges and hoaxes.

The School recognises the crucial role it plays in relation to preventative education and that this is most effective in the context of a whole school approach that prepares pupils for a life in modern Britain and creates a culture of zero tolerance for sexism, misogyny/misandry, homophobia and sexual violence and sexual harassment.

Pupils are also taught about the risks associated with all forms of abuse, including physical abuse and sexual violence and sexual harassment which may include an online element. The School has a zero tolerance approach to sexual violence and sexual harassment and such behaviour is never acceptable and will not be tolerated. The School will treat any such incidences as a breach of discipline and will deal with them under the School's Behaviour and Discipline Policy and also as a safeguarding matter under the School's Safeguarding and Child Protection Policy and procedures.

The School recognises that effective education needs to be tailored to the specific needs and vulnerabilities of individual pupils, including those who are victims of abuse, and those with special educational needs and disabilities, and this is taken into account when devising and implementing processes and procedures to ensure the online safety of its pupils.

Parents

The School is in regular contact with parents and carers and uses communications to reinforce the importance of ensuring that children are safe online. The School aims to help parents understand what systems are in place to filter and monitor their child's online use.

Useful online safety resources for parents:

(a) https://www.saferinternet.org.uk/advice-centre/parents-and-carers
(b) http://www.childnet.com/parents-and-carers
(c) https://www.nspcc.org.uk/preventing-abuse/keeping-children-safe/onlinesafety/
(d) https://www.thinkuknow.co.uk/parents/

(e) https://www.thinkuknow.co.uk/parents/articles/theres-a-viral-scare-onlinewhat-should-i-do/
(f) http://parentzone.org.uk/
(g) https://www.internetmatters.org/
(h) https://www.commonsensemedia.org/
(i) Advice for parents and carers on cyberbullying (DfE, November 2014)
(j) https://www.askaboutgames.com/
(k) https://www.ceop.police.uk/safety-centre
(l) https://safeblog.lgfl.net/2018/11/parents-scare-or-prepare

Inappropriate Material

Any inappropriate websites or material found by pupils or school personnel will be reported to the Head Teacher who in turn will report to the Internet Service Provider.

Filtering and monitoring

Whilst considering their responsibility to safeguard and promote the welfare of pupils and provide them with a safe environment in which to learn, the SLT will do all it reasonably can to limit pupils' exposure to risks from the School's IT system. As part of this process, the School has appropriate filtering and monitoring systems in place and regularly reviews their effectiveness.

The School has regard to Government filtering and monitoring standards, which require that the School:

- Identifies and assigns roles and responsibilities to manage filtering and monitoring systems;
- Reviews filtering and monitoring provision at least annually;
- Blocks harmful and inappropriate content without unreasonably impacting teaching and learning; and
- Has effective monitoring strategies in place that meet their safeguarding needs.

Security of LPEBL Internet system

- The SLT has ensured that appropriate filters and monitoring systems are in place and meet the DfE's filtering and monitoring standards and is mindful that this should not lead to unnecessary restrictions on learning.
- New programs will be installed onto the network or stand alone machines by authorised personnel only.
- **Personal memory sticks, CD's and other data recording devices may not be used in school.**
- Everyone must be aware that under the Computer Misuse Act 1990, the use of computer systems without permission or for inappropriate use, could constitute a criminal offence.

Reviewing this E-Safety Policy

The effectiveness of this policy will be reviewed by the Head Teacher on an annual basis. In line with new technologies the necessary recommendations for improvement will be made to the proprietors.