LONDON WELSH SCHOOL
YSGOL GYMRAEG LLUNDAIN

E-SAFETY POLICY

Prepared: April 2016

Adopted: September 2016

Reviewed: March 2019

YSGOL GYMRAEG LLUNDAIN

LONDON WELSH SCHOOL

E-Safety Policy 2019 -2021

Policy Reviewed - March 2019

Next Review – March 2019

1. Mission

We strongly believe that our school has an integral role in keeping children safe in the community and when using technology. Our aim is to ensure that children can explore and develop their skills, knowledge and understanding to the fullest potential in a safe, nurturing and inclusive environment, which includes the wider community and on the internet.

We recognise that ICT and the internet are beneficial tools for learning and communication that can be used in school to enhance the curriculum, challenge students, and support creativity and independence. However, it is important that the use of the internet and ICT is seen as a responsibility and that students, staff and parents use it appropriately and practise good e-safety. It is important that all members of the school community are aware of the dangers of using the internet and how they should conduct themselves online. We aim to offer the best possible provision and protection for all children in our care, with due regard to the evolving nature of technology.

2. Compliance

This policy complies with government guidance and advice on E-Safety *'Advice on Child Internet Safety 1.0; Universal guidance for providers' (DfE, UKCCIS, 2012)* and written with reference to the following documents:

- Disability Act 2010
- Equality Act 2010
- YG Anti-Bullying Policy
- YG Safeguarding Policy
- YG Accessibility Policy and Plan
- DfE Keeping Children Safe in Education (2018)
- Staff Code of Conduct
- GDPR 2018

This policy is available from the school office and on the school website for parents, staff, and pupils to access when and as they wish. Rules relating to the school code of conduct when online, and e-safety guidelines, are displayed around the school. E-safety is integrated into the curriculum in any circumstance where the internet or technology are being used. PSHE Education lessons teaches E-safety where personal safety, responsibility, and/or development are being discussed.

3. Definitions

As outlined in the above documents, 'E-Safety' encompasses protection whilst operating the following within a school context, setting or wider community where appropriate;

- Internet Technologies e.g. e-mail, world wide web
- Electronic communications e.g. mobile phones

4. Aims and Objectives

We aim to provide simulative environments and access to technology within our school which is relevant to the child and the real world. This is to support children's learning and with the outcome expected for children to be responsible and active members of the community. Technology offers a wide range of resources, information and knowledge which supports education and general administration systems on a daily basis. Whilst we acknowledge the beneficial use of technology in operating our school, we are aware of the continually developing nature of technology. We consequently strive to ensure our provision protects children and staff whilst operating technology, and that procedures are in place in the case of an incident or an at-risk situation, both inside and outside of school.

Our objectives to achieve are outlined below.

1. A designated teacher is appointed as the E-Safety Co-ordinator.
   The School e-Safety Coordinator is Miss Sioned Jones
   The designated member of the governing body responsible for e-safety is Jonathan Wright.
2. Offer provision of a recognised internet service provider (ISP) with age-related filtering.
3. All teaching and non-teaching staff are aware and able to recognise e-safety issues.
4. Established a clear reporting processes in the case of an incident.
5. Support and advice offered to parents to ensure e-safety is a priority in school and at home.
6. Encourage open, honest and safe communication between pupils and staff to prevent any potential harm or risks. Such risks are made aware to parents, pupils and staff, with support networks available as needed.
7. Priority given to training, and continuation training, to all staff, including the contribution of the wider school community.

5. Making use of ICT and the internet in school

The internet is used in school to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our students with all the necessary ICT skills that they will need in order to enable them to progress confidently into a professional working environment when they leave school.

Some of the benefits of using ICT and the internet in schools are:

For pupils:

- Access to worldwide educational resources and institutions such as art galleries, museums and libraries.
- Contact with schools in other countries resulting in cultural exchanges between pupils all over the world.
- Access to subject experts, role models, inspirational people and organisations.
- An enhanced curriculum; interactive learning tools; collaboration, locally, nationally, and globally; self-evaluation; feedback and assessment; updates on current affairs as they happen.
- Access to learning whenever and wherever convenient.
- Freedom to be creative.
- Freedom to explore the world and its cultures from within a classroom.
- Social inclusion, in class and online.

- Access to case studies, videos and interactive media to enhance understanding.
- Individualised access to learning.

For staff:

- Professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies.
- Immediate professional and personal support through networks and associations.
- Ability to communicate effectively with parents through email.
- Class management, schedules, and assignment tracking.

6. Authorised Internet Access

- All staff must read and sign the 'ICT: Acceptable Use Agreement' upon recruitment, and are aware before using any school ICT resource.
- Parents are informed upon pupil entry that they will be provided with supervised Internet access to enhance lessons and learning. They will be asked to sign and return a consent form for pupil access.
- Posters are displayed surrounding technological resources and equipment as a reminder of internet access guidelines and safe use of online use.
- Restrictions are in place on all laptops to restrict unauthorised and unsuitable websites.
- Provision of a recognised internet service provider (ISP) with age-related filtering is in place to restrict unauthorised and unsuitable websites.
- Should staff or pupils discover unsuitable sites, the URL address, time, content must be reported to the Designated E-Safety Officer.
- School will ensure that the use of Internet derived materials by pupils and staff complies with copyright laws.
- Pupils to be taught how to critically validate information online before accepting its accuracy, and to be aware of plagiarism when using.

7. E-Mail

The school uses email internally for staff and pupils, and externally for contacting parents, and is an essential part of school communication. It is also used to enhance the curriculum by:

- initiating contact and projects with other schools nationally and internationally
- providing immediate feedback on work, and requests for support where it is needed.

Staff and pupils should be aware that school email accounts:

- Should only be used for school-related matters, i.e for staff to contact parents, students, other members of staff and other professionals for work purposes. This is important for confidentiality.
- Staff should only use official school-provided email accounts to communicate with pupils, parents or carers. Personal email accounts should not be used to contact any of these people.
- Emails sent from school accounts should be professionally and carefully written. Staff are representing the school at all times and should take this into account when entering into any email communications. At times it may be necessary to authorise an email before sending, in the same way as a headed letter.

- Staff must tell a member of the senior leadership team if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves.
- The sending of chain letters using school account is prohibited.
- Pupils may only use approved e-mail accounts on the school system
- Pupils must not reveal any personal information over email.
- Pupils will be educated through the ICT curriculum to identify spam, phishing and virus emails and attachments that could cause harm to the school network or their personal account or wellbeing.

8. Published Content

The school website is viewed as a useful tool for communicating our school ethos and practice to the wider community. Ofsted also requires schools to provide information for our stakeholders on line. It is also a valuable resource for parents, students, and staff for keeping up-to-date with school news and events, accessing school policies, prospectus, celebrating whole-school achievements and personal achievements, and promoting school projects.

- The website is in the public domain, and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the school community, copyrights and privacy policies.
- School website should contain school address, e-mail and telephone number but should not contain staff or pupil personal information.
- Designated E-Safety teacher will take overall editorial responsibility and ensure that content is accurate and appropriate.
- For the pupil corner section, blogs will be written offline by pupils and monitored and evaluated by the Designated E-Safety teacher for approval online.
- Work and/or photographs which include pupils need to be carefully selected and comply with parental permission consent. Staff must ensure that photographs of pupils does not refer to their names. Under the GDPR 2018 images of pupils and staff will not be displayed in public, either in print or online, without consent. On admission to the school parents/carers will be asked to sign a photography consent form.

Parents should follow standard school complaints procedure if they have a concern or complaint regarding the misuse of school photographs. Please refer to our complaints policy for more information on the steps to take when making a complaint. Any issues or sanctions will be dealt with in line with the schools child protection and safeguarding policy and behaviour policy.

9. Social Networking and Personal Publishing.

Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes.

These online forums are the more obvious sources of inappropriate and harmful behaviour, cyber bullying, peer on peer abuse and contextual abuse (Keeping children safe in education, 2018), and where pupils are most vulnerable to being contacted by a dangerous person. It is important that we educate students so that they can make their own informed decisions and take responsibility for their conduct online.

Students are taught through the ICT curriculum and PSHE Education about the risks and responsibility of uploading personal information and the difficulty of taking it down completely once it is out in such a public place. The school follows general rules on the use of social media and social networking sites in school:

- Pupils are educated on the dangers of social networking sites and how to use them in safe and productive ways. They are all made fully aware of the school's code of conduct regarding the use of ICT and technologies and behaviour online.
- Any sites that are to be used in class will be risk-assessed by the teacher in charge prior to the lesson to ensure that the site is age-appropriate and safe for use.
- Pupils and staff are encouraged not to publish specific and detailed private thoughts, especially those that might be considered hurtful, harmful or defamatory. The school expects all staff and pupils to remember that they are representing the school at all times and must act appropriately.
- Safe and professional behaviour of staff online will be discussed at staff induction.
- Pupils are continually advised on personal details, photos and other identification information on their personal accounts and the consequent risks.
- Pupils and staff are also advised on security and password safety.

10. Mobile Phones

While mobile phones and personal communication devices are commonplace in today's society, their use and the responsibility for using them should not be taken lightly. The school will not tolerate cyberbullying against either pupils or staff.

- Under no circumstances should staff use their own personal devices to contact pupils or parents either in or out of school time.
- Staff are not permitted to take photos or videos of pupils. If photos or videos are being taken as part of the school curriculum or for a professional capacity, the school equipment will be used for this.
- The school expects staff to lead by example. Personal mobile phones should be switched off or on 'silent' during school hours and kept in a secure location in the office unless in an emergency situation.
- Any breach of school policy may result in disciplinary action against that member of staff.

11. Bullying

Our ethos is to promote tolerance and independence in all our pupils throughout our curriculum, and we continue to be aware of peer on peer abuse, sexual harassment online, cyber bullying and contextual abuse (Keeping Children Safe in Education, 2018). Further information is available in our Anti-Bullying policy. Refer to Appendix I for **definitions of current e-safety issues.**

Cyberbullying, as with any other form of bullying, is taken very seriously by the school. Information about specific strategies or programmes in place to prevent and tackle bullying are set out in the behaviour policy. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the school community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

If an allegation of bullying does occur, the school will:

- act as quickly as possible to establish the facts. It may be necessary to examine school systems and logs or contact the service provider in order to identify the bully
- record and report the incident
- provide support and reassurance to the victim
- make it clear to the 'bully' that this behaviour will not be tolerated. If there is a group of people involved, they will be spoken to individually and as a whole group. It is important that children who have harmed another, either physically or emotionally, redress their actions and the school will make sure that they understand what they have done and the impact of their actions.

If a sanction is used, it will correlate to the seriousness of the incident and the 'bully' will be told why it is being used. They will be asked to remove any harmful or inappropriate content that has been published, and the service provide may be contacted to do this if they refuse or are unable to remove it. They may have their internet access suspended in school.

Repeated bullying may result in a fixed-term exclusion.

12. Information System Security

- School ICT systems capacity and security will be reviewed regularly
- Virus protection will be installed and updated regularly

13. E-Safety Incident

The school will follow a rigorous procedure in the event of an E-Safety incident or at-risk situation is identified (e.g. access to unauthorised site is granted, cyber-bullying, risk of grooming).

Refer to Appendix I for **definitions of current e-safety issues.**

14. Storing and Managing Information

We take responsibility for ensuring that any data that we collect and process is used correctly and only as is necessary, and the school will keep parents fully informed of the how data is collected, what is collected, and how it is used. National curriculum results, attendance and registration records, special educational needs data, and any relevant medical information are examples of the type of data that the school needs. Through effective data management we can monitor a range of school provisions and evaluate the wellbeing and academic progression of our school body to ensure that we are doing all we can to support both staff and students.

Information and documents are stored in line with the government guidance under GDPR 2018 on keeping and maintaining records. Please refer to 'Gov.UK: Keeping and Maintaining Records' for further information.

15. Training and Resources

Provision for the training is funded through the school's central fund. As needed, training for staff is either provided within school or through the Local Educational Authority's programme. Training aims to address the understanding and potential strategies and programmes to aid young learners.

16. Complaints Procedure

In the event of a complaint against the school, the processes within the Complaints Policy will be followed.

Appendix 1:

Overarching e-safety risks and definitions
Definitions of current e-safety issues

Inappropriate content: It is possible that children may come across things online which are inappropriate for their age and stage of development. In school filters and restriction settings on particular devices are used to block this content.

Cyberbullying[1] is the act of bullying others over the internet or on a mobile phone by sending abusive emails or texts directly or by posting nasty comments or humiliating images for others to see. Like any form of bullying, cyberbullying can be horrible for the children involved and hard for them to talk about. Cyber bullying is a new form of bullying. Cyber-bullying is a new way to describe common forms of bullying such as name- calling, racism, homophobia, sexism etc.

Online grooming Pupils may meet people online who aren't who they say they are. This could take place in a game online (Many games now are linked to the internet and players across the globe.) Grooming is a word used to describe people befriending children in order to take advantage of them for sexual purposes.
Grooming usually takes place over a long period of time. In cases of sexual predators and radicalization, friendships with unsuspecting children are built up over a time span of 2-3 years.

Sexual abuse: Involves forcing or enticing a child or young person to take part in sexual activities, ... whether or not the child is aware...The activities may...include non-contact activities, such as involving children in look at, or in the production of, sexual images, watching sexual activities, encouraging children to behave in sexually inappropriate ways, or grooming a child in preparation for abuse (including via the internet). Sexual abuse is not solely perpetrated by adult males. Women can also commit acts of sexual abuse, as can other children.

Sexting [1]The term 'sexting' is used to describe the sending and receiving of sexually explicit photos, messages and video clips, by text, email or posting them on social networking sites. Young people increasingly choose to send images and messages to their friends, partners, or even strangers they meet online.
Sexting can be defined as:
'The exchange of sexual explicit messages' and 'creating, sharing and forwarding sexually suggestive or nearly nude images' through mobile phones/devices and the internet'

- **by children under the age of 18**
- **or of children under the age of 18**

Online reputation The internet keeps a record of everything we do online – the photos we upload, the comments other people make about us and things we buy. This is our online reputation. It's important that children and adults understand how to manage their online reputation and the impacts for them of a negative online reputation.

Self harm[1] Self-harm is often understood to be a physical response to an emotional pain of some kind, and can be very addictive. Some of the things people do are quite well known, such as cutting, burning or pinching, but there are many ways to hurt yourself, including abusing drugs and alcohol or having an eating disorder. People who self-harm often say it provides short-term relief to emotional pain.

Extremism [1]The vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and the mutual respect and tolerance of different faith and beliefs. We also regard calls for the death of members of our armed forces as extremist.

Radicalisation a child may meet people online or visit websites that could lead them over time to adopt extreme right-wing views, and become radicalised. Curiosity could lead a child to seek out these people. As in the incidence of online grooming, an adult online could befriend a child in order to encourage them to adopt beliefs or persuade them to join groups whose views and actions are considered extreme.

Appendix 2:

E-Safety Rules

These E-Safety Rules help to protect pupils and the school by describing acceptable and unacceptable computer use.

- The school owns the computer network and can set rules for its use.
- It is a breach of school rules for staff, pupils and volunteers to use the computer or network for a purpose not permitted by the school.
- Irresponsible use may result in the loss of network or Internet access.
- Network access must be made via the user's authorised account and password, which must not be given to any other person.
- All network and Internet use must be appropriate to education.
- Copyright and intellectual property rights must be respected.
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers.
- Anonymous messages and chain letters are not permitted.
- Users must take care not to reveal personal information through email, personal publishing, blogs or messaging.
- The school ICT systems may not be used for private purposes, unless the head teacher has given specific permission.
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

Appendix 3:

Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the school's e-safety policy for further information and clarification.

- The information systems are school property and I understand that it is a breach of school rules to use a computer for a purpose not permitted by its owner.
- I will ensure that my information systems use will always be compatible with my professional role.
- I understand that school information systems may not be used for private purposes, without specific permission from the Lead Teacher.
- I understand that the school may monitor my information systems and Internet use to ensure policy compliance.
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager.
- I will not install any software or hardware without permission.
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- I will respect copyright and intellectual property rights.
- I will report any incidents of concern regarding children's safety to the school e-Safety Coordinator or the Designated Child Protection Coordinator.
- I will ensure that any electronic communications with pupils are compatible with my professional role.
- I will promote e-safety with pupils in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The school may exercise its right to monitor the use of the school's information systems, including Internet access, the interception of e-mail and the deletion of inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: ……………………………… Capitals: ……………………… Date: ………

Accepted for school: ……………………………. Capitals: …………………………