Poplar Primary School online safety policy 2019

As a Rights Respecting school (Articles 13, 16 & 17) we aim to ensure that children stay safe online at school and develop the awareness to be safe online at home.

1a. Aims
● To safeguard and protect the children and staff of Poplar Primary School.
● To ensure that children understand how to be safe and responsible online and that they develop an awareness of their digital footprint.
● To ensure that children and staff know to whom they should report concerns.

1b. Key Objectives:
● set clear expectations of behaviour and codes of practice for responsible use of the Internet and other devices such as handheld devices (AUP policies)
● have clear structures to deal with online abuse such as cyberbullying which are cross-referenced with other school policies (safeguarding).
● ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable (AUP and behaviour policies).
● To develop an understanding that trustworthy and untrustworthy sources of information and opinions exist online (through modelling and teaching).

1c. Areas of risk
● exposure to inappropriate content, including online pornography, ignoring age ratings in games.
● hate sites
● content validation: how to check authenticity and accuracy of online content
● photo sharing without permission
● grooming
● cyber-bullying through all devices and platforms including social media.
● identity theft (including ‘frape’ (hacking Facebook profiles)) and sharing passwords
● privacy issues, including disclosure of personal information
● digital footprint and online reputation
● health and well-being (amount of time spent online (Internet or gaming))
● sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
● copyright (little care or consideration for intellectual property and ownership – such as music and film)

1d. Agreed Procedures
● The school will use an approved internet filtering system.
● The school will reinforce the message that social media sites have minimum age requirements and can involve significant online dangers.
Poplar Primary School online safety policy 2019

- The school reinforces that age ratings for games etc. are there to protect children and so should not be ignored.
- Staff will receive suitable training in online safety.
- Staff will embed online safety training as part of lessons as it is an integral part of the Computing curriculum.
- Staff will report any online concerns to the safeguarding lead and inclusion manager.
- Online incidents will be logged using a record of concern sheet.
- Ensure that users may only access the school’s networks through an authorised and properly enforced password protection policy.
- Virus protection will be kept up to date.
- Children will be made aware of the laws around copyright.
- All data held on pupils on the school computers will have appropriate access controls in place.
- All pupils will be supervised when engaged in learning activities involving online technology including extra-curricular and extended school activities.
- Children and parents sign AUPs.
- Information regarding online safety to be shared at class talks.

1e. Is this working?

- Children will understand the importance of reporting abuse, misuse or access to inappropriate materials
- Children will know what action to take if they or someone they know feels worried or vulnerable when using online technology.
- Children will know and understand school policy on the use of mobile phones, digital cameras and handheld devices.
- Children will know and understand school policy on the taking / use of images and on cyber-bullying.
2. Education and Curriculum

2a. Pupil online safety curriculum

This school

Has a clear, progressive online safety education programme as part of the Computing curriculum / PSHE curriculum. It is built on LA / LGfL online-safeguarding and e-literacy framework for EYFS to Y6/ national guidance. This covers a range of skills and behaviours appropriate to their age and experience, including:

- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign/will be displayed throughout the school/will be displayed when a student logs on to the school network.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include: risks in pop-ups; buying online; online gaming / gambling;

2b. Staff and governor training

This school

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes training available to staff and governors on online safety issues and the school’s online safety education programme.
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the e-safeguarding policy and the school’s Acceptable Use Policies.

2c. Parent awareness and training

This school

- Provides advice, guidance and training for parents, including:
  - Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear
  - Information leaflets; in school newsletters; on the school website;
  - Demonstrations, practical sessions held at school;
  - Suggestions for safe Internet use at home;
  - Provision of information about national support sites for parents.
3. Expected Conduct and Incident management

3a. Expected Conduct
In this school, all users have agreed to an Acceptable Use Policy (AUP).

3b. Incident Management
In this school:
- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions.
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school’s escalation processes.
- support is actively sought from other agencies as needed (e.g. the local authority and regional broadband grid, UK Safer Internet Centre helpline) in dealing with online safety issues.
- monitoring and reporting of online safety incidents takes place and contribute to developments in policy and practice in online safety within the school. The records are reviewed/audited and reported (where appropriate) to the school’s senior leaders, Governors/the LA / LSCB (London Safeguarding Children’s Board).
- parents / carers are specifically informed of online safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law.

3c. Password Policy
- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it;
- All staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private.
- We require staff to use STRONG passwords for access into our MIS system.

4. E-mail

4a. This school
- Provides staff with an email account for their professional use, and makes clear personal email should be through a separate account;
- Does not publish personal e-mail addresses of pupils, staff or governors on the school website.
- Will contact the Police if one of our staff or pupils receives an e-mail that we consider is particularly disturbing or breaks the law.
Poplar Primary School online safety policy 2019

- Will ensure that email accounts are maintained and up to date
- Reports messages relating to or in support of illegal activities to the relevant Authority and if necessary to the Police.
- Knows that spam, phishing and virus attachments can make e-mails dangerous. We use a number of LGfL-provided technologies to help protect users and systems in the school, including desktop anti-virus product, plus direct email filtering for viruses, Trojans, pornography, phishing and inappropriate language. Finally, and in support of these, LGfL WebScreen2 filtering monitors and protects our Internet access to the World Wide Web.

4b. Pupils:
- We use Gmail with pupils.
- Pupils are introduced to, and use e-mail as part of the ICT/Computing scheme of work.
- Pupils are taught about the safety and ‘netiquette’ of using e-mail both in school and at home.
- Pupils sign the school Agreement Form to say they have read and understood the online safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

4c. Staff:
- Staff can only use the LA or Gmail systems on the school system
- Staff only use LA or Gmail systems for professional purposes
- Access in school to external personal e-mail accounts may be blocked
- Never use email to transfer staff or pupil personal data. We use secure, LA / DfE approved systems. These include: S2S (for school to school transfer); Collect; USO-FX, named LA system;
- All staff sign our LA / school Agreement Form AUP to say they have read and understood the online safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

5. Google Apps for Education
- Uploading of information on the schools’ Learning Platform / virtual learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas;
- Photographs and videos uploaded to the schools learning platform will only be accessible by members of the school community;
- In school, pupils are only able to upload and publish within school approved and closed systems, such as Google drive.
6. Video Conferencing

This school only uses the LGfL video conferencing / skype with adult supervision.

7. Equipment and Digital Content

8. Personal mobile phones and mobile devices

Staff and students must abide by relevant AUP

Date approved: Jan 2019

Date for review: Autumn 2020