E-Safety/Online Safety Policy

Oliver Goldsmith Primary

"Inspiring a love of learning."

Date Ratified: September 2019

Date to be reviewed: September 2020

1. Introduction

1.1 At Oliver Goldsmith Primary School we understand the responsibility we have to educate our pupils on e-safety issues; teaching them appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.
1.2 Oliver Goldsmith Primary School has a whole school approach to the safe use of ICT and creating this safe learning environment includes three main elements:

- An effective range of technological tools
- Policies and procedures, with clear roles and responsibilities
- A comprehensive e-safety programme for pupils, staff and parents.

1.3 This policy has been contributed to by the whole school and ratified by the governors.
1.4 This policy is to be read in conjunction with all other policies particularly: Keeping Children Safe in Education 2019, Working together to Safeguard Children 2018, Behaviour Policy, Safeguarding and Child Protection Policy, Code of Conduct Policy, Inclusion Policy and Equality Policy.

2. Roles and Responsibilities

2.1 E-Safety is recognised as an essential aspect of everyone's role.
2.2 All teachers are responsible for promoting and supporting safe behaviours in their classrooms and follow school e-safety procedures.
2.3 All staff should be familiar with the school's policy including:

- Safe use of e-mail
- Safe use of the internet
- Safe use of the school network, equipment and data
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras
- Publication of pupil information/photographs on the school website
- Procedures in the event of misuse of technology by any member of the school community (see appendices)
- Their role in providing e-safety education for pupils.

2.4 Staff are reminded/updated about e-safety regularly and new staff receive information on the school's acceptable use policy as part of their induction.

3. Curriculum

3.1 Computing and online resources are increasingly used across the curriculum.
3.2 We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis.
3.3 We continually look for new ways to promote e-safety:

- We provide opportunities within a range of curriculum areas to teach about e-safety.
- Educating pupils on the dangers of technologies that may be encountered outside school is done informally, when opportunities arise and as part of the curriculum.
- Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling, and activities as part of the ICT curriculum.
- We regularly distribute questionnaires to children to monitor their understanding of e-safety.
- Pupils are aware of the impact of online bullying through PSHE and know how to seek help if they are affected by these issues. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies.
- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum

4. Managing Internet Access

4.1 The internet is an open communication medium, available to all, at all times.
4.2 Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education as well as a potential risk to young people.

4.3 Pupils will have supervised access to internet resources through the school's fixed and mobile internet technology.
4.4 Staff will preview any recommended sites before use.
4.5 Raw image searches are discouraged when working with pupils.
4.6 If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher.
4.7 It is advised that parents recheck these sites and supervise any further research.
4.8 Our internet access is controlled through the London Grid for Learning (LGFL) web filtering service.
4.9 Staff and pupils are aware that school-based email and internet activity can be monitored and explored further if required.
4.10 If staff or pupils discover an unsuitable site, the screen must be switched off/closed and the incident reported immediately to the e-safety co-ordinator/DSL and an email sent to the network manager so that they can block the site.
4.11 It is the responsibility of the school, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up-to-date on all school machines.
4.12 Any changes to filtering must be authorised by a member of the senior leadership team.

5. Security and Data Protection

5.1 The school and all staff members comply with the Data Protection Act 1998.
5.2 Personal data will be recorded, processed, transferred and made available according to the act.
5.3 Password security is essential for staff, particularly as they are able to access and use pupil data.
5.3 Staff have secure passwords which are not shared with anyone.
5.4 All users read and sign an Acceptable Use Policy to demonstrate that they have understood the school's E-Safety Policy.
5.5 Children and parents will sign the AUP when they start in Reception (EYFS/KS1 AUP) and then in Year 3 (KS2 AUP) and then be reminded of it annually at the start of each academic year.
5.6 Staff will sign their AUP every 3 years and will be part of the induction for new staff.
5.7 All new children, parents and staff will sign when they start school.

6. E-Safety Complaints/Incidents

6.1 As a school we take all precautions to ensure e-safety at all times. However, due to the international scale and linked nature of internet content, the availability of mobile technologies and the speed of change, it may mean that unsuitable material may briefly appear on a computer or mobile device. The school cannot accept liability for material accessed or any consequences of this.
6.2 Complaints should be made to the Headteacher. Incidents should be logged and the flowchart for managing an e-safety incident is to be followed.
6.3 It is important that the school work in partnership with pupils and parents to educate them about cyber bullying and children, staff and families need to know what to do if they or anyone they know are a victim of cyber bullying.
6.4 All bullying incidents will be recorded and investigated (see Behaviour Policy for more information).

7. Review of Policy

7.1 There are on-going opportunities for staff, children and families to discuss e-safety concerns with our Learning Mentors.
7.2 This policy needs to be reviewed every year and consideration given to the implications for future whole school development planning.
7.3 The policy will be amended if new technologies are adopted or any guidance or orders are updated.