

## **Online Safety Policy**

### **Introduction**

Maryland Primary School is committed to safeguarding and ensuring that pupils are able to access the internet safely in school and understand how to keep themselves safe online out of school.

The Online Safety Policy should be read in conjunction with the Safeguarding, Behaviour and Anti-Bullying policies.

### **Online safety within the curriculum**

All pupils are taught how to keep themselves safe online through Computing lessons as well as timetabled assemblies and CPSHE Enrichment days.

Pupils will be taught:

- How to use ICT safely to support their learning in school
- How to use technology safely outside of school
- What to do if they feel unsafe or unhappy when using technology

Pupils will always be taught at an age appropriate level and objectives will be taken from the 'Digital Literacy' strand of the Computing National Curriculum. Our scheme of work is based on the 'Education for a Connected World' framework produced by the UK Council for Child Internet Safety (UKCCIS).

### **Managing online safety risks within school**

The internet is an essential element of education and the school has a duty to provide pupils with quality internet access as part of their learning experience. The school ensures that appropriate filtering systems are used. The school's internet access is regulated by LGFL (London Grid For Learning). The internet access we provide is a 'managed' system rather than a 'locked down' system, in accordance with Ofsted 2014 guidance that these allow pupils with the opportunities to learn how to assess and manage risk for themselves. Governors and Senior Leaders conduct internet filter checks termly.

### **Online safety agreements**

All pupils agree to a set of online safety rules at the beginning of the academic year and sign to show their agreement. If pupils break any of these rules, they may receive sanctions in line with the school's behaviour policy. In situations where pupils repeatedly break the online safety rules or there is a serious breach, they may be temporarily banned from using the school's technology.

All members of staff sign an online safety agreement and a code of conduct.

### **Working in partnership with parents**

We understand the importance of working closely with parents and aim to keep parents informed about online safety. All parents sign their agreement to the school's online safety rules in the home-school agreement. We also keep parents and carers informed of online safety issues via:

- The school website (including the CEOP button where they can report concerns directly to the police)
- Newsletter updates and reminders
- Online safety workshops

### **Dealing with online safety incidents**

Concerns about online safety should be referred to the Computing lead and a Designated Safeguarding Leader in the first instance. These members of staff will investigate the incident, including interviewing pupils and staff where necessary. Parents and carers will be informed about online safety incidents involving their children and advised about how to prevent further incidents. Where incidents involve a possible breach of the law, the police will be informed.

The school may investigate online safety issues that take place outside of school, in line with our safeguarding requirements and our commitment to anti-bullying.

Any concerns regarding a member of staff's use of the internet should be referred to the Headteacher, in accordance with whistleblowing procedures.

### **Training**

All staff members will be trained on online safety annually, as part of their safeguarding training. It is the responsibility of the Computing Lead to keep up to date with changes to technology and online safety risks and inform staff of any changes.

### **Roles and Responsibilities**

This table details the roles and responsibilities of staff and governors.

<b>Role</b>	<b>Key Responsibilities</b>
Senior Leadership Team	<ul style="list-style-type: none"><li>• To take overall responsibility for online safety provision</li><li>• To take overall responsibility for data and data security</li><li>• To be responsible for ensuring that staff receive suitable training</li><li>• To be aware of procedures following a serious online safety incident</li></ul>
Computing Lead	<ul style="list-style-type: none"><li>• To keep up to date with online safety legislation and issues and cascade to staff</li><li>• To take responsibility for the online safety curriculum</li></ul>

	<p>and schemes of work and monitor the delivery of this</p> <ul style="list-style-type: none"> <li>• To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident</li> <li>• Facilitate training for staff and parents</li> <li>• Liaise with the school technician</li> </ul>
Governors	<ul style="list-style-type: none"> <li>• To approve the Online Safety Policy and review the effectiveness of the policy</li> </ul>
Teachers	<ul style="list-style-type: none"> <li>• Teach online safety lessons, following the timetable and schemes of work provided by the Computing Lead</li> </ul>
Technician	<ul style="list-style-type: none"> <li>• To report any online safety related issues that arise to the Computing Lead and Senior Leaders</li> <li>• To ensure that access controls/encryption exists to protect sensitive information</li> </ul>

All other staff, including Children's Centre Staff, private providers and volunteers must adhere to the online safety policy and online safety agreement.

**January 2019**