E-Safety Policy for Springfield Infant School

Springfield is a Rights Respecting school.

Article 3- The best interests of the child must be a top priority in all actions concerning children.

Article 12 – Every child has the right to say what they think in all matters.

Article 28 – Every child has the right to an education.

Article 29 – Every child has the right to develop their personality, talents and abilities.

Introduction

Our aim in presenting an e-safety policy is to create a safe environment where we can all work and learn. This environment should be safe for both young people and adults alike.
E-safety is not purely a technological issue. The responsibility for e-safety must not be solely delegated to technical staff, or those with a responsibility for IT.
Schools must therefore, firmly embed e-safety within all safeguarding policies and practices. This then makes that responsibility rest with of all those who work with young people whether in a paid or unpaid capacity.
No one policy or technology can create the safe learning and working environment we need. Schools can work towards this by combining the following:

1. **Policies** and Guidance.
2. **Technology** Based Solutions
3. **Education** in terms of acceptable use and responsibility

Policies

The policies and guidance to help form safe environments to learn and work in include, but are not limited to:

- The school Acceptable Use Policy (AUP)
- The school Internet Filtering Policy
- The staff Guidance for the Safer Use of the Internet

These policies set the boundaries of acceptable use. Schools need to use these policies however in conjunction with other policies including, but not limited to:

- The Behaviour for learning and Anti –bullying policy
- The Staff Handbook / Code of Conduct for Staff

Technology

The technologies to help form a safe environment to learn and work include:

- Internet filtering – Our IT company provide an up-to-date and high quality internet filtering solution.
- Antivirus Software – regularly updated and may be supplied by the School's IT Support Team (SITST).

- Schools may also decide to use "Automatic network monitoring software" including, but not limited to, products such as Securus or Policy Central.
-

Education

The education of young people is key to them developing an informed confidence and resilience that they need in the digital world.

The National Curriculum programme for IT at Key Stages 1 to 4 makes it mandatory for children to be taught how to use IT safely and securely. Together these measures form the basis of a combined learning strategy that can be supported by parents, carers, and the professionals who come into contact with children.

Educating young people in the practice of acceptable use promotes responsible behaviour and builds resilience. Relationships and Health Education (RHE) lessons can also provide an opportunity to explore potential risks, how to minimize these and to consider the impact of our behaviour on others.

We cannot realistically provide solutions to each and every potential issue arising in a rapidly changing world. As a result, young people must be able to transfer established skills and safe working practices to any new "e-activities" they encounter.

We recognise that it is equally important to ensure that the people who care for young people should have the right information to guide and support young people whilst empowering them to keep themselves safe.

E-Safety Incident report form is to be used by all teachers or staff members if required. See appendix.

Mr Ben Miller, ICT technician from Homefield Primary School, is responsible for our computing hardware and software, and provides technical support and advice to all staff. He can be contacted by email on itsupport@homefield-primary.co.uk .

E-safety Incident Report

This Event Report Form Compiled By: Name Title Date	
Staff informed: Name & Date Headteacher e-safety co-ordinator Child protection officer Other	
Nature of Concern: Who was involved: pupil/staff/parents?	
Where did it occur: home, school?	
Time and date of Incident:	
Time and date the incident was logged:	
Action taken: (please tick)	

Evidence preserved Senior staff informed Other action	
Incident witnessed by: Staff Pupil Parent Other	
Other Officers Involved in Response: LA Officer LADO NCC Network Security Manager Other	
Follow up Action:	
Evidence Collected (and where retained):	
Review Date if required:	