



# Little Reddings School policy

Little Reddings Primary School  
Harcourt Road, Bushey,  
Watford, Herts  
WD23 3PR  
Tel: 0208 950 5388  
Fax: 0208 420 548  
Headteacher: Miss Carly Simmonds

Little Reddings Primary School  
E-safety Policy 2014

### **Vision**

For our school community to develop their computing skills safely and understand their responsibilities for using technology in their lives.

### **Introduction and rationale**

With the ever changing and exciting possibilities that new technology brings, there are also many safety and responsibility issues that must be addressed. Our school community's development of safe and responsible technology use is vital.

### **Aims**

Embedded within our community's use of technology, there must be an understanding of how they as users need to keep themselves safe as well as an understanding of their own personal responsibilities.

### **Objectives**

- To use internet services appropriately and respectfully.
- To react appropriately when concerned with online communication.
- To be aware of the importance of password safety.
- To have an awareness of copyright law when using technologies.
- To use school data in line with data protection and confidentiality procedures.
- To use images of the children with consent of their parents and carers.

### **Planning for teaching and learning**

Our safety message is embedded throughout the Hertfordshire computing scheme of work taught from the Foundation Stage through to Upper Key Stage 2. These themes are placed in context through the use of the VLE, online CEOP resources, online discussions and through story telling appropriate to each year group.

Our implementation of the VLE gives our children the opportunity to communicate with peers in a safe password protected online environment, only assessible to our school community. Within this safe domain, our children have been given the responsibility to report any social networking activity that concerns them by using the embedded whistle blowing facility.

Our children's concerns have previously included unkind posts, password misuse, and inappropriate age related blogs. We believe, in a world where cyber bullying has become an increasing issue in people's lives, teaching children to respond to and manage the misuse of technology by others has become increasingly important.

When an issue is reported, a discussion will follow within the school with individuals or whole class as appropriate. Initially, these discussions aim to guide the use of respectful and responsible communication, however if such issues continue sanctions will be applied linked to the Simply Behave policy.

If a repeated behaviour concerns other members of our school community, a child's account may be blocked as a sanction and parents and carers will be informed. Once an agreed period of time has passed, a child's account will be reactivated so they can swiftly take the opportunity to learn from previous issues.

### **Assessment and recording**

The assessment of children's capacity in e-safety is one element which is taken into consideration when children's computing levels are monitored over time, as specified within the Hertfordshire scheme of work.

An ongoing e-safety log is updated within the administration facility of our VLE. Here a record of children's 'whistle blowing' is kept. If a student's online behaviour has impacted on their daily Simply Behave chart, a written report to parents/carers would be included.

### **Equal opportunities and special needs in ICT**

All children regardless of ethnicity, gender, disability or physical ability will be given equal access to work and equipment. Based on our class surveys and information from the Mind the Gap study, we have provided lunch time 'access for all' clubs to ensure internet access for all children. This gives all our children access to ongoing work on our school's VLE.

### **Roles and responsibilities**

The computing coordinator will organise the development of the policy and co-ordinate training to support policy aims. This will ensure the balanced delivery of e-safety across the curriculum; monitor the implementation of the scheme of work; evaluate classroom practise in the use of VLE and regularly disseminate aspects of good practise to staff.

The computing coordinator will offer weekly internal VLE training, run incidental INSET/Staff meetings and manage the VLE.

Class teachers will be responsible for reading the ICT policy document and implementing it into their classrooms. When needing help or advice they will ask the co-ordinator.

It is the joint responsibility of class teachers and computing coordinator to monitor the use of the VLE and respond to whistle blowing.

The responsibility of communicating the safety message to our school community is primarily that of the computing coordinator, although the e-safety message should be reinforced by the class teacher within a PSHE context. The e-safety awareness message is spread through parent/carer consultation, parental presentations, staff meetings, insets and reporting to governors.

Our school infrastructure operates a WF3 filter for child accessed network profiles and a WF1 filter for staff use. Any inappropriate images that are accessed through our school filters are reported to the computing coordinator. In response, our technical support team at Bushey Meads block the specific URL that is hosting the inappropriate image. If an image is of an extreme nature, we will then report the incident to county to investigate the source of the material.

The use of children's images are only permitted in public domains with consent of parents or carers. Use of such images within our VLE is permitted as this service is only accessible through passwords within our school community.

The storage of children's images or confidential school data on external servers is in line with county's requirements for external storage (see data protection policy.)

Any concerns of the misuse of school technology by any member of our school community should be reported to the computing coordinator or head teacher.

Password security is the responsibility of individual members of our community. Any concerns of password security breach should be reported to the computing coordinator.