Upper Beeding Primary School

E – Safety Policy

December 2013

Introduction

Our aim in presenting an e-safety policy is to create a safe environment where we can both 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 ICT.
Schools must, therefore, firmly embed e-safety within all safeguarding policies and practices. This then makes that responsibility rest with all of 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 Acceptable Use Policy (AUP)
- The West Sussex Internet Filtering Policy
- The Staff Guidance for the Safer Use of the Internet
- The Information Security Guidance

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 and Anti-Bullying Policy
- The Staff Handbook
- Professional Standards

Technology

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

- Internet Filtering – The Local Authority has deployed a system approved by central government agencies (Becta). In addition to this, schools may deploy local filtering that only affects their own network as an option available from the LA. Alternatively they might add a separate extra filter "on top" of the LA solution.

- Antivirus Software – regularly updated and usually supplied by the Schools 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 ICT at Key Stages 1 to 4 makes it mandatory for children to be taught how to use ICT 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. Personal, Social and Health Education (PSHE) 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.

If you have any queries please contact either Simon Gawn, ICT in Schools Officer, on 01243 777926 or email: ictinschools@westsussex.gov.uk

(adapted from the policy issued by West Sussex)
Reviewed, Adopted and Ratified by:

Staff	December 2013
Governing Body	Next Behaviour and Safety Committee meeting Jan/Feb 2014

Date for Review December 2016