Birdham CE Primary School
E-SAFETY POLICY

Introduction
A safe electronic environment 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. This then makes that responsibility rest with of all those who work with young people whether in a paid or unpaid capacity.

Aims
- to create a safe environment where we can both work and learn. This environment should be safe for both young people and adults alike.
- to embed e-safety within all safeguarding policies and practices.

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. To support this, the following procedures are in place:
- e-Safety rules are posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils are informed that network and Internet use will be monitored and appropriately followed up.
- e-Safety training will be embedded within the ICT scheme of work or the Personal Social and Health Education (PSHE) curriculum.

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.

Policies
The policies and guidance to help form a safe environment to learn and work in include, but are not limited to:
- the Acceptable Use Policy (AUP);
- the TrustNET Internet Filtering Policy;

- photographic images of children guidelines;
- the staff guidance for the safer use of the internet; and
- information security guidance.
- These policies set the boundaries of acceptable use. Copies can be found in the PPA room. They have links with other school policies such as:
- behaviour management policy;
- anti-bullying policy; and
- staff handbook and code of conduct for staff

Writing and reviewing the e-safety policy

- The e-Safety Policy is part of the School Improvement Plan and relates to other policies including those for ICT, bullying and for child protection.
- The ICT co-ordinator (with support from the ICT Technician) has the role of e-Safety Coordinator. The e-Safety Coordinator works closely with the member of staff responsible for Child Protection, which at Birdham CE Primary School is the Headteacher . N.B. The e-Safety Coordinator is not a technical role.
- Our e-Safety Policy has been written by the school, building on the West Sussex e-Safety Policy and government guidance. It is shared with all staff and approved by governors.

Teaching and learning at Birdham CE Primary School

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils. Internet use will enhance learning
- Birdham CE Primary School Internet access has been designed expressly for pupil use and will include filtering appropriate to the age of pupils.
- Pupils are taught what kind of Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- Pupils are shown how to publish and present information to a wider audience. Pupils are taught how to evaluate Internet content
- The school will ensure that the use of Internet derived materials by staff and pupils complies with copyright law.
- Pupils are taught the importance of cross-checking information before accepting its accuracy.
- Pupils are taught to report unpleasant Internet content to the Headteacher, or their class teacher who will share this information with the e-Safety Coordinator so that a path of action can be agreed.

Managing Internet Access at Birdham CE Primary School
Information system security

- School ICT systems security are reviewed regularly.
- Virus protection is updated regularly.

E-mail

- Pupils may only use approved e-mail accounts on the school system.
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- In e-mail communication, pupils must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated with care and attachments not opened unless the author is known.
- The school does not encourage e-mail from pupils to external bodies unless the contact is well known.
- The forwarding of chain letters is not permitted.

Published content and the school web site

- Pupils details are not available on the website.
- The headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupil's images and work

- Photographs that include pupils will be selected carefully with the permission of parents/guardians.
- Pupils full names will not be used with their photographs anywhere on the school Web site or other online space.
- Work can only be published with the permission of the pupil and parents/carers.
- Parents are clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories. Social networking and personal publishing
- The school filters do not allow access to major social networking sites. Pupils are taught how to use messaging via secure systems, including secure class Kidblog accounts, which is moderated.
- Pupils are advised never to give out personal details of any kind which may identify them, their friends or their location.
- Pupils and parents are advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.
- Pupils are advised to use nicknames and avatars when using social networking sites.

Managing filtering

- The school works with TrustNET and other e-safety sites to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable online materials, the site must be reported to the e-Safety Coordinator.
- Pupils will work with a supervising teacher when making or answering a video conference call.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The school understands that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications, e.g. staff mobile phones. Pupil mobile phones are not permitted in school. The sending of abusive or inappropriate messages is forbidden.
- The use by pupils of cameras in mobile phones will be kept under review.
- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.

Protecting personal data

- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

Authorising Internet access

- All staff must read and sign the "Staff AUP Agreement for ICT" before using any school ICT resource.
- The school will maintain a current record of all staff and pupils who are granted access to school ICT systems.
- At Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form. Any person not directly employed by the school will be asked to sign an "Acceptable Use Agreement" before being allowed to access the internet from the school site.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the school network. Neither the school nor West Sussex County Council can accept liability for any material accessed, or any consequences of Internet access.
- The school will audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff.
- Any complaint about staff misuse must be referred to the headteacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure (see schools complaints against the curriculum policy).
- Pupils and parents will be informed of consequences for pupils misusing the Internet.

Introducing the e-safety policy to pupils

- e-Safety rules will be posted in all rooms where computers are used and discussed with pupils regularly.
- Pupils will be informed that network and Internet use will be monitored and appropriately followed up.
- e-Safety training will be delivered as part of the ICT and PSHE curriculum.

Staff and the e-Safety policy

- All staff will be given the School e-Safety Policy and its importance explained.
- 'Safer Practice with Technology for Adults working with Children', provides more details for adults at school to be aware of in order to ensure everyone is 'eSafe'.
- Staff must be informed that network and Internet traffic can be monitored and traced to the individual user.
- Staff that manage filtering systems or monitor ICT use will be supervised by the Headteacher and work to clear procedures for reporting issues.
- Staff will always use a child friendly safe search engine when accessing the web with pupils.

Enlisting parents' and carers' support

- Parents and carers attention will be drawn to the School e-Safety Policy in newsletters, the school prospectus and on the school Web site.
- The school will maintain a list of e-safety resources for parents/carers.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child with the school.

External media on portable devices

- Staff and children should be aware of the associated risks of connecting devices to networks outside the school, and the possible harm that any downloaded files might bring.

The 360° safe – (an e-safety self review tool)

The school uses the 360° safe self-review tool provided by the South West Grid for Learning. It is intended to help schools review their e-safety policies and practice.