Heene Church of England (Aided) Primary School

E-Safety Policy

Date Approved: **May 2016**

This Policy has been agreed by the senior leadership team and approved by the Full Governing Body

1. Introduction

Heene Church of England Primary School takes the safety of our pupils very seriously which includes safety while using computers and electronic internet enabled devices. E-safety includes pupils, staff and governors making the best use of computing in a safe manner and learning about being safe online.

E-safety is the protection and education of staff and children in their use of technology, in particular the internet. It provides a safe working environment within which staff can work and children can learn.

The E-safety policy will operate in conjunction with other school policies including:

- Behaviour policy
- Anti-bullying policy
- Child protection policy
- PHSE policy
- Curriculum policy
- Data protection and Security
- The Staff Handbook/Code of Conduct for Staff

2. Teaching and learning

Heene Church of England (aided) Primary School has a duty to teach children how to use ICT safely and securely as part of their education and learning experience. Internet access is part of the statutory curriculum and a necessary tool for staff and children. Access to the computers is supervised at all times and all school computers are designed with age appropriate tools on each year group log-in. All computers/tablets currently have a filtering service Surfprotect which is installed by JSPC, which includes e-safety benefits such as more control over children's viewing and notifications can be sent to the head of e-safety if certain words are used on computers.

Pupils are taught what internet use is acceptable and what is not and given clear objectives for internet use. Pupils are taught to be critically aware of the materials they read and are shown how to validate information before accepting its accuracy.

As part of the new computing curriculum, all year groups have digital literacy units that focus on different elements of staying safe online. These topics include how to use a search engine, our digital footprint and cyber bullying.

3. Managing internet access

3.1 Information system security

- The security of the ICT systems within Heene Church of England (aided) Primary School is reviewed regularly.
- The school will work with the DfES and JSPC computer service to ensure that systems to protect pupils are reviewed and improved.
- Virus protection is updated regularly.
- If staff or pupils discover an unsuitable site, it must be reported immediately to the E-safety Coordinator and JSPC technician.
- The E-safety Coordinator or senior manager should ensure that regular checks are made to ensure that the filtering methods are appropriate and effective.
- Any portable devices should have a virus check before being used on the internet on the network in school.
- If any administrator account passwords become known they will be changed straight away.
- Computers, including mobile phones, may not be connected to the school network or Wi-Fi without specific permission.

3.2 Email

- Staff have access to approved Heene Primary email accounts at school.
- **Our current cohorts are not old enough to require their own emails and this will be reviewed when they are, if it is appropriate. They may have their own E-Schools accounts but must be taught about safe use and must tell an adult if they receive offensive mail.**
- Incoming emails should be treated with care and attachments not opened unless the author is known.

3.3 Published content and school website

- The contact details on the school website are the school address, email and telephone number. Staff and governor names and job roles are published. Pupil's personal details are not published.
- The head teacher has overall editorial responsibility and ensures that content is accurate and appropriate.
- Photographs that include pupils are selected carefully so they do not enable individual children to be clearly identified, unless parental permission has been given.
- Pupil's full names are not used anywhere on the school website.
- Written permission from parents or carers must be obtained before photographs of pupils are published on the school website.

3.4 Social networking and personal publishing

Social networking internet sites provide facilities to chat and exchange information online. The online world is very different from the real one with the temptation to do and say things that would not be done if you were face to face.

- The use of social networking sites in school is prohibited for students and is blocked by our filters.
- Pupils are taught not to give out personal details of any kind that may identify themselves, other pupils, their school or location. This also includes photographs and videos.
- Pupils and parents will be advised that the use of social network sites outside of school is inappropriate for primary aged children.
- Pupils are encouraged to only interact with known friends, family and staff over the internet and deny access to others.
- Parents, pupils and staff are advised of the dangers of discussing pupils, staff or the school on social networking sites. The governors will consider taking legal action, where appropriate, to protect pupils and staff against cyber bullying and defamatory.

3.5 Mobile phones/Electronic devices

- Currently students are not allowed mobile phones in school and if they are found to have one they are to be locked in a cupboard in the office and can be collected by their parent or guardian at the end of the school day.
- Parents and guardians will be advised that the children will not be able to bring mobile phones or any device with internet or phone access into school.
- This will be reviewed by senior management and governors as the school expands and the pupils become older.

3.6 Cameras and videos

Although most cameras are not directing linked to the internet, the images can easily be transferred.

- Publishing of photographs and videos will follow the guidelines set out in sections 3.3 and 3.4 of this policy.
- Parents may use cameras to take images of their own child in school plays/assemblies when a member of senior management gives permission but they must not take images of other children. Images of children taken in school must not be shared on social networking sites.

4. Managing emerging technologies

Technology is fast changing and developing and Heene Primary School will endeavour to keep up with new technologies as much as possible within the financial constraints that schools are faced with. As new technology comes to the forefront, this school will consider it with regards to the educational benefit that it could bring. A risk assessment will be carried out before use in school is allowed.

5. Protecting personal data
   - Personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998 and Freedom of Information Act.

6. Assessing risks
   - The school takes all reasonable precautions to ensure that users access only appropriate material using JSPC's Surfprotect filtering system.
   - The school audits ICT provision on an annual basis to establish if the e-safety policy is adequate and that its implementation is effective.
   - Methods to identify, assess and minimize ricks will be reviewed regularly.

7. Handling e-safety complaints
   - Complaints of internet misuse will be dealt with by the head teacher or a senior member of staff in their absence.
   - Any complaint about staff misuse must be referred to the head teacher or governing body.
   - Complaints of a child protection nature will be dealt with in accordance with school protection procedures.
   - Pupils and parents will be informed of the complaints procedure.
   - Discussions will be held with Sussex Police to establish procedures for handling potentially illegal issues.

8. Policy Decisions

8.1 Authorising internet access

- All staff must read and sign the 'Acceptance ICT Use Agreement' before using any school ICT resource.
- The School will keep a record of all staff and pupils who are granted internet access. The record will be kept up to date, for example a member of staff may leave or a pupil's access to the internet may be withdrawn.
- At Key stage 1 access to the internet will be by adult demonstration with supervised access to specific, approved on-line materials.
- Parents will be asked to sign and return a consent form.

8.2 Introduction of E-safety to staff members

- All staff have copies of the school's E-safety Policy and know its importance.
- Staff are aware that Internet traffic can be monitored and traced to the individual user.

8.3 Introduction of E-safety to pupils

- E-safety rules are posted in all networked rooms and discussed with the pupils at the start of each year.
- Pupils are informed that the network and Internet use will be monitored.
- E-safety will also be introduced to the children through the provision of information to their parents and carers. In the first instance, this will be by bringing the parents attention to the school's E-safety Policy. This will be done via the school website, prospectus and newsletter.

Georgia Bearcroft