POLICY FOR E - Safety

1. School Aims and Values

The School's Aims are:

- To serve its pupils by providing an education of the highest quality within the context of Christian belief and practice.
- To create a learning community where pupils are encouraged to learn in a creative, innovative and challenging way.
- To provide a rich and varied curriculum that enables all pupils to acquire, develop and apply a broad range of knowledge, understanding and skills.
- To create a positive school community where everyone is respected and valued.
- To make learning fun.
- To work with parents and the local community to strengthen the partnerships of learning.

Aims for E - Safety

The purpose of this policy is to:

- establish the ground rules we have for using the Internet and electronic communications, such as mobile phones, collaboration tools and personal publishing. It highlights the need to educate pupils about the benefits and risks of using technology and provides safeguards and awareness for users to enable them to control their online experience.
- describe how these fit into the wider context of our Behaviour, Safeguarding and Child Protection policies.
- demonstrate the methods used to protect children from sites containing pornography, racist or politically extreme views and violence.

Objectives

E-Safety encompasses the use of new technologies, internet, social networking, and electronic communications such as mobile phones, collaboration tools and personal publishing.
The school's e-safety policy will operate in conjunction with other policies including those for Bullying, Child Protection, Curriculum, Data Protection and Security.

E - Safety depends on effective practice at a number of levels. This policy aims to ensure that there is;

- responsible ICT use by all staff and students; encouraged by education and made explicit through published policies.

- sound implementation of the E-safety policy in both administration and curriculum, including secure school network design and use.
- safe and secure internet access, including the effective management of filtering.
- the appointment of an E-Safety Coordinator to implement and monitor this policy. (Head teacher and ICT Subject Leader)

Inclusion and Equal Opportunities

George Fentham Endowed School is keen to enable every child to have the support he or she needs to be healthy, stay safe, enjoy and achieve, make a positive contribution and achieve economic well being.

Each child is valued and respected regardless of ability, race, gender, religion, social background, culture or disability and is offered a child-centered curriculum, opportunities to develop to their full potential, the means to develop physically, intellectually, emotionally and socially and the chance to develop good behaviour and responsible attitudes for life.

Staff ensure their approach to all children is non-discriminatory, that all groups have equal access to the full range of educational opportunities provided by the school and that diversity is celebrated.

Teaching and Learning/ Implementation

The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students 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.
- the school Internet access is designed expressly for pupil use and includes filtering appropriate to the age of pupils.
- pupils are taught what Internet use is acceptable, and what is not, and given clear objectives for Internet use (National Curriculum/E Safety Curriculum).
- pupils are educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation
- the school ensures that the use of Internet derived materials by staff and pupils complies with copyright law.
- pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.

Managing Access

- school ICT systems capacity and security is 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.
- pupils must not reveal personal details of themselves, or others, in e-mail communication, or arrange to meet anyone – in the real or on-line/virtual world.
- e-mail sent to an external organisation must be authorised before sending, in the same way as a letter written on school headed paper.

School web site/Extranet site

- the contact details on the Web site and/or Extranet site should be the school address, e-mail and telephone number. Staff or pupils' personal information is 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 pupils to be clearly identified (image and name will never appear together).
- pupils' full names are not used anywhere on the Web site/Extranet.
- written permission from parents or guardians is obtained before photographs of pupils are published on the school Web site/Extranet *(see separate permissions in E-Safety file).*
- pupil's work will only be published with the permission of the pupil and parents/guardians.

Social networking and personal publishing

- the school blocks access to social networking sites.
- newsgroups are also blocked.
- pupils are told never to give out personal details of any kind which may identify them
- pupils and parents are advised that the use of social network spaces outside school is inappropriate for primary aged pupils.
- Staff will not communicate with pupils through private email accounts or social networking sites, on educational matters, but will use official email and networking sites sanctioned by the school. Staff will be circumspect in their use of social networking sites and will not discuss school business or school issues on their personal social networking site.
- Staff MUST not accept either pupils or ex-pupils as 'friends'.

Managing filtering

- if staff or pupils discover an unsuitable site, it must be reported immediately to the E-Safety Coordinator.

- senior staff make regular checks to ensure that the filtering methods selected are appropriate and effective (Filtering/Firewall and Anti-Virus - Sophos - are provided/maintained by Solihull LA, alongside SB & Schools ICT Technician).

Managing videoconferencing

- videoconferencing uses the educational broadband network to ensure quality of service and security rather than the Internet.
- pupils must ask permission from the supervising teacher before making or answering a videoconference call.
- videoconferencing is appropriately supervised for the pupils' age.

Managing emerging technologies

- emerging technologies are examined for educational benefit and a risk assessment is carried out before use in school is allowed.
- mobile phones are not to be used during school time. The sending of abusive or inappropriate text messages is forbidden.

Managing the Use of Personal Technology

- Staff, and children, will not use their personal mobile phone, camera (still or moving images) or other devices to take, edit or store images of pupils/staff from this school. An exception to this practice will be that **named staff may be authorised by the Head Teacher** to bring their own camera into school, without a memory card. Any images taken for school business will be recorded onto a school memory card. All images will only be stored, edited or archived onto school equipment.
- Mobile phones and personal devices will not be used during lessons or formal school time. They should be switched off at all times.
- Mobile phones will not be used during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from the Head Teacher.
- The Bluetooth function of a mobile phone should be switched off at all times and not be used to send images or files to other mobile phones.
- Electronic devices of all kinds that are brought in to school are the responsibility of the user. The school accepts no responsibility for the loss, theft or damage of such items. Nor will the school accept responsibility for any adverse health effects caused by any such devices either potential or actual.
- If a pupil or member of staff breaches the school policy then disciplinary action may be taken.

Protecting personal data

- personal data is recorded, processed, transferred and made available according to the Data Protection Act 1998.

Managing Cyber-Bullying

Cyberbullying can be defined as "The use of Information Communication Technology, particularly mobile phones and the internet, to deliberately hurt or upset someone" DCSF 2007

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policy on Child Protection (including anti-bullying and behaviour).
- There are clear procedures in place to support anyone in the school community affected by cyberbullying. (See Child Protection/Anti-Bullying/Behaviour Policies)
- There are clear procedures in place to investigate incidents or allegations of Cyberbullying. (See Child Protection/Anti-Bullying/Behaviour Policies)
- All incidents of cyberbullying reported to the school will be recorded.
- Pupils, staff and parents/carers will be advised to keep a record of the bullying as evidence.
- The school will take steps to identify the bully, where possible and appropriate. This may include examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers will be required to work with the school to support the approach to cyberbullying and the school's e-Safety ethos.

Sanctions for those involved in cyberbullying can include:

- The bully being asked to remove any material deemed to be inappropriate or
- A service provider being contacted to remove content, if the bully refuses or is unable to delete content.
- Internet access being suspended at school for the user for a period of time.
- Parent/carers of pupils being informed.
- The Police being contacted, if a criminal offence is suspected.

(Other sanctions for pupils and staff may also be used in accordance with the schools Child Protection, anti-bullying, behaviour policies or Acceptable Use Policy.)

Policy decisions

Authorising Internet access

- all staff read and sign the 'Acceptable ICT Use Agreement' before using any school ICT resource.
- the school keeps a record of all staff and pupils who are granted Internet access. The record will be kept up-to-date, for instance if a member of staff leaves or a pupil's access be withdrawn.

- at Key Stage 1, access to the Internet will be by adult demonstration with directly supervised access to specific, approved on-line materials.
- at Key Stage 2, access to the Internet will be by supervised access to specific, approved on-line materials.
- parents are asked to sign and return a photographic permissions form.
- parents and pupils are asked to sign and return an 'Acceptable ICT Use Agreement'. (see separate permissions in E-Safety file)

Assessing risks

- the school takes all reasonable precautions to ensure that users access only appropriate material by using the Solihull Local Authority 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.

Handling E-safety complaints

- complaints of Internet misuse are dealt with by a senior member of staff/e-safety co-ordinator.
- any complaint about staff misuse are referred to the head teacher.
- complaints of a child protection nature are dealt with in accordance with the school's child protection procedures, including referral to the DMS (Reference is made in the Child Protection Policy directly to E-Safety).
- pupils and parents are informed of the complaints procedure.

Communications

Introducing the E-safety policy 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 network and Internet use will be monitored.
- as part of our Safeguarding routines, Key Stage 2 pupils and their parents are informed of the child exploitation and online protection centre: thinkuknow.co.uk

Staff and the E-Safety policy

- 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.

Enlisting parents' support

- parents' attention is drawn to the school's E-Safety Policy in newsletters, the school brochure, E – Safety workshops and on the school Web site/Extranet.

Monitoring/Role of Subject Leader

The coordination, implementation and monitoring of e-safety is the responsibility of the subject leader, e-safety co-ordinator and head teacher. The subject leader and e-safety co-ordinator also:

- Support colleagues by keeping them informed about current developments in E-safety, and by providing a strategic lead and direction for this area.
- Give the head teacher an annual summary report in which s/he evaluates the strengths and weaknesses in e-safety, and indicate areas for further improvement.
- Use specially allocated regular management time to review the curriculum and policies and to assess implementation and impact across the school.

Background Documentation

This policy was informed by reference to;

- BECTA www.becta.org.uk/
- CEOP (Child Exploitation and Online Protection) www.ceop.gov.uk/
- LCP: Policies for Primary Schools.
- www.kenttrustweb.org.uk
- Consultation with SIAS ICT Team.
- George Fentham Endowed School Child Protection/Behaviour Policy 2014
- Solihull LA E – Safety Policy (Appendix 1)
- www.thinkyouknow.co.uk

The date for review of this policy is …….

Signed by …….

Date ……